2019

Effects of Correlation of Channel Gains on the Secrecy Capacity in the Gaussian Wiretap Channel

Abhishek Lokur
University of Nebraska - Lincoln, abhilokur94@gmail.com

EFFECTS OF CORRELATION OF CHANNEL GAINS ON THE SECRECY CAPACITY IN THE GAUSSIAN WIRETAP CHANNEL

by

Abhishek Pradeep Lokur

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of the Requirements

For the Degree of Master of Science

Major: Telecommunications Engineering

Under the Supervision of Professor H. Andrew Harms

Lincoln, Nebraska

July, 2019

EFFECTS OF CORRELATION OF CHANNEL GAINS ON THE SECRECY CAPACITY IN THE GAUSSIAN WIRETAP CHANNEL

Abhishek Pradeep Lokur, M.S.

University of Nebraska, 2019

Advisor: H. Andrew Harms

Secrecy Capacity is one of the most important characteristic of a wiretap channel in wireless communication systems. Therefore, the study of this characteristic wherein the system has correlated channel gains and study them for different line-of-sight (LOS) propagation scenarios is of ultimate importance.

The primary objective of this thesis from the mathematical side is to determine the secrecy capacity for correlated channel gains for the main and eavesdropper channels for the Gaussian Wiretap channel as a function from main parameters (μ, Σ, ρ). $f(h_1, h_2)$ is the joint distribution of the two channel gains at channel use (h_1, h_2), $f_i(h_i)$ is the main distribution of the channel gain h_i. The results are based on assumption of the Gaussian distribution of channel gains (g_M, g_E). The main task of estimating the secrecy capacity is reduced to the problem of solving linear partial differential equations (PDE). Different aspects of the analysis of secrecy capacity considered in this research are the estimation of Secrecy Capacity mathematically and numerically for correlated SISO systems and a mathematical example for MIMO systems with PDE.

The variations in Secrecy Capacity are studied for Rayleigh (N-LOS) distribution and Rician (LOS) distribution. Suitable scenarios are identified in which secure communication is possible with correlation of channel gains. Also, the new algorithm using PDE has a higher speed than analog algorithms constructed on the classical statistical Monte-Carlo methods. Taking into account the normality of the distribution of system parameters, namely the channel gain (g_M, g_E), the algorithm is constructed for systems of partial differential equations which satisfies the secrecy criterion.

ACKNOWLEDGMENTS

First and foremost, I wish to express my sincere gratitude to my thesis advisor, Dr. H. Andrew Harms of the Electrical & Computer Engineering Department at University of Nebraska-Lincoln. I will always be indebted to him for his timely guidance, recommendations, research experiences and facilities during my thesis writing and graduate school. From the start of my graduate school, I gained the opportunity to be a Graduate Researcher for Dr. Harms, which has molded me academically and provided a solid platform to display my academic and research credentials.

I would like to thank and appreciate my career advisor, Dr. Hamid Sharif of the Electrical & Computer Engineering Department at University of Nebraska-Lincoln for his guidance in every semester of my program which helped me utilize my knowledge and skills to the best of their potential.

I would like to thank my thesis defense committee, Prof. Won Mee Jang and Dr. Lamar Yang of the Electrical & Computer Engineering Department at University of Nebraska-Lincoln, in addition with Dr. Harms, for investing their time in reviewing my thesis and providing me positive future directions for my work.

Additionally, I wish to thank the administrative staff in UNL's Department of Electrical & Computer Engineering. A special acknowledgement towards the College of Engineering and the University of Nebraska for providing me the opportunity and the facilities to fulfill my Masters.

Finally, I am forever indebted to my parents who are my pillars of strength; a thank you would not suffice. A big thank you to all my friends from whom I am always gaining valuable experiences and to all the people who have contributed towards this thesis directly and indirectly.

Table of Contents

List of Figures **vi**

List of Tables **viii**

List of Abbreviations **x**

List of Symbols **xi**

1 Introduction & Wireless Security Background **1**

1.1 State-of-the-art Wireless Security 1

1.2 Relationship between Entropy and Mutual Information 4

1.2.1 Entropy: Statistical Approach 4

1.2.2 Mutual Information 4

1.3 Channel Capacity and Secrecy Capacity 5

1.3.1 Channel Capacity 5

1.3.2 Secrecy Criterion – Secrecy Capacity 7

1.4 Information Theoretic Secrecy: Theory & Real World Problems 8

1.5 Correlation of Channel Gains 9

1.6 Main Results & Contributions 12

1.7 Other Generalizations of the Main Model 15

1.8 Thesis Outline 19

2 History of Physical Layer Security & Related Works **20**

2.1 Security at the Physical Layer 20

2.2 Physical Layer Security over the Years 21
2.2.1 Shannon's Cipher System 21
2.2.2 Wyner's Wiretap Channel 22
2.2.3 Gaussian Wiretap Channel & the MIMO Wiretap Channel 24
2.3 Importance of the Available CSI at Transmitter 26
2.4 Literature Review 27
2.5 Summary 32

3 Fading Gaussian Wiretap Channel with Correlation of Channel Gains 34
3.1 Non-Convexity of the Secrecy Capacity Expression 34
3.2 Bounds on Secrecy Capacity over Correlated Fading Channels with Full CSI 35
3.3 Expected Secrecy Capacity with Correlation of Channel Gains: Using PDE . 41
3.3.1 SISO Systems 41
3.3.2 MIMO Systems 47

4 Theoretical & Numerical Results 51
4.1 Expected Secrecy Capacity with Correlation of Channel Gains using Monte-Carlo Method 51
4.2 Comparison of Expected Secrecy Capacity using Monte-Carlo method & PDE for Correlated Channel Gains 53

5 Conclusions 61
5.1 Future Work 62

Bibliography 63

List of Figures

1.1 Gaussian Wiretap Channel 2
1.2 The joint density $f(h_1, h_2)$ plot for different values of correlation coefficient $\rho = -0.9, -0.5, 0, 0.99$. 11
1.3 Grid of the points in the (μ_1, μ_2) plane for estimation of the secrecy capacity C_S 14

2.1 Shannon's model of a secrecy system. 22
2.2 Wyner's wiretap channel 23

4.1 Contour plot of Secrecy Capacity as function of correlation ρ and SNR 52
4.2 Contour plot of the secrecy capacity C_S as function of the parameters (μ_1, μ_2) calculated by MC method 54
4.3 Contour plot of the secrecy capacity C_S as function of the parameters (μ_1, μ_2) calculated by PDE from Eqn. (3.12) 55
4.4 Contour plot of the secrecy capacity C_S as function of the parameters $(\sigma_1, \sigma_2) \in [0, 10]^2$ calculated by PDE 57
4.5 Contour plot of the secrecy capacity C_S as function of the parameters $(\rho, SNR) \in [-1, 1] \times [0, 5]$ for different values of (μ_1, μ_2) and for constant SNR at the Eavesdropper 58
4.6 Contour plot of the secrecy capacity C_S as function of the parameters $(\rho, SNR) \in [-1, 1] \times [0, 5]$ for the values $(\mu_1 = 0, \mu_2 = 1)$ and for constant SNR at the Eavesdropper 59

4.7 Contour plot of Secrecy Capacity as function of correlation ρ and signal-to-noise ratio SNR for N-LOS propagation with varying SNR at the receiver and constant SNR at the eavesdropper 60

List of Tables

1.1 Existing ways of estimation of C_S for different systems 3

2.1 Main results of estimation of C_S for different system 33

4.1 Execution time for MC and PDE algorithms 53

List of Abbreviations

Abbreviations	Explanation
AWGN	Additive White Gaussian Noise
BC	Broadcast Channel
BC-CM	BC with Confidential Messages
CDF	Cumulative Distribution Function
CSI	Channel State Information
C_S, SC	Secrecy Capacity
DE	Differential Equation
MC	Monte Carlo method
MIMO	Multiple Input Multiple Output
MaMIMO	Massive MIMO
MISO	Multiple Input Single Output
MGBC-CM	Multi-Antenna Gaussian BC with Confidential Messages
MMSE	Minimum Mean Square Error
OSI	Open Systems Interconnection
PDE	Partial Differential Equation
PDF	Probability Density Function
RCI	Regularized Channel Inversion
SDPC	Secret Dirty Paper Coding
SIMO	Single Input Multiple Output
SINR	Signal-to-Interference-plus-Noise-Ratio
SISO	Single Input Single Output system
SNR	Signal-to-Noise Ratio

List of Symbols

- X or X^n – Input signal (Alice signal);
- Y or Y^n – Legitimate output signal (Bob signal);
- Z or Z^n – Eavesdropper output signal (Eve signal);
- n – Length of signal X;
- m – Length of signal Y;
- k – Length of signal Z;
- $N = n(m + k)$ – Number of parameters in the system;
- g_M – Channel gain between X and Y, $m \times n$ matrix;
- g_E – Channel gain between X and Z, $k \times n$ matrix;
- μ – Average values of (g_M, g_E), $N \times 1$ vector;
- Σ – Covariance matrix for (g_M, g_E), $N \times N$ matrix;
- ρ – Correlation vector of the parameters of system (g_M, g_E), $N \times N$ matrix
- $h = (h_1, h_2)$ – Realization of the channel gains (g_M, g_E);
- $\sim$ – Distributed by (density, mass function/ probability law);
- n_M – Additive Gaussian noise in legitimate channel, $m \times 1$ random process;
- n_E – Additive Gaussian noise in eavesdropper channel, $m \times 1$ random process;

- f, p_X – density of the random variable;
- $f_{\mu,\Sigma}$ – density of the Gaussian random variable with average values μ and covariance matrix Σ;
- $H(X)$ – entropy of the random variable X;
- $H(X|Y)$ – conditional entropy of the random variable X by random variable Y;
- $P(x, y)$ – probability $P(X = x \text{ and } Y = y)$;
- P_{error} – probability of the error in the channel;
- $Tr(A)$ – trace of the matrix A;
- $diag(a_1, ..., a_n)$ – $n \times n$ matrix with diagonal elements $a_1, ..., a_n$, where all other non-diagonal elements are 0;
- $\Delta f(x)$ – increment of the function f in point x;
- $\|x - y\|$ – Euclidean distance between x and y;
- $det(A)$ – determinant of the matrix A;
- $O(f)$ – asymptotic notation regard function f;
- $C_S^{lim}(dist)$ – asymptotic value of the secrecy capacity for $SNR \to \infty$ for distribution $dist$;
- $A \to B, A \Rightarrow B$ – channel between A and B.

Chapter 1

Introduction & Wireless Security Background

1.1 State-of-the-art Wireless Security

The widely used mathematical solutions for analyzing the operation of transmission channels, taking into account the presence of an eavesdropper, are random processes and random variables that allow accurate determination of the basic characteristics of communication channels. In this research, the same approach will be used – the simulation of transmission systems in the capacity of random processes.

Another important factor to be considered is the presence of uncertainty, which describes the "undeterministic" components of any model. This model considered contains two sources of uncertainty:

1. The uncertainty of the model itself.

2. Existence of the random noises in the wireless physical layer.

These will be described using *random variables* and *random processes*, namely:

1. Uncertainty of the model by assumption, that coefficients of the model are random variables;

2. Random noises in the wireless physical layer by Additive White Gaussian Noise (AWGN) in the channel.

For defining nature of the randomness, the standard notation $RV \sim f(F)$ will be used, where this notation means that the random variable RV has density f (distributed by probability law F[1]).

It can be argued that the protection of information (or minimization of the possibility of loss of information) is one of the most important tasks in any organization or company. In this study, the AWGN Wiretap channel which is described below in Fig. 1.1 is considered:

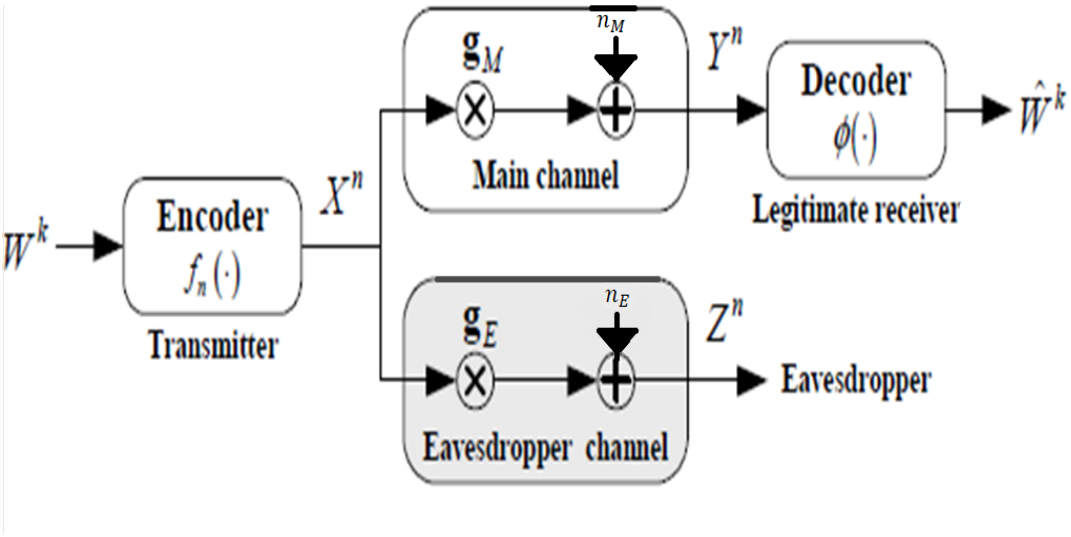

Figure 1.1: Gaussian Wiretap Channel

where parameters of the system are:

- X^n, the input parameter (signal) of the system – vector of the order $n \times 1$;
- g_M, g_E, the channel gains of the main and eavesdropper channels respectively – matrices of the size $m \times n$ and $k \times n$ respectively;
- n_M, n_E are independent and identically distributed (i.i.d.) Gaussian noises with zero mean and unit variance – m and k dimensional Gaussian processes.

The mathematical model of the channel in Fig. 1.1 is given by

[1]For example, F in normal distribution $N(0,1)$.

$$\begin{cases} Y^n = g_M X^n + n_M, \\ Z_n = g_E X^n + n_E. \end{cases} \tag{1.1}$$

Many authors in their works [8, 9, 35, 37, 38, 39, 41, 42] use separation of the model by SISO, SIMO, MISO and MIMO by the following notations of the coefficients:

- g_M, g_E, n_M, n_E for SISO systems;
- $\mathbf{g_M}, \mathbf{g_E}, \mathbf{n_M}, \mathbf{n_E}$ for MISO and SIMO systems;
- $\mathbf{G_M}, \mathbf{G_E}, \mathbf{N_M}, \mathbf{N_E}$ for MIMO and MaMIMO systems.

These designations will not be used, but instead the dimensions of the matrices g_M, g_E and vectors n_M, n_E will be determined. Note that finding a closed form for C_S is a difficult task, and this form is not found for all cases. The main methods for finding this indicator are described in the table below:

System	Existing of closed form	Method of estimation C_S
SISO	Yes	Monte Carlo methods; DE
MISO	Particularly	Monte Carlo methods
SIMO	No	Monte Carlo methods
MIMO	No	Monte Carlo methods
Correlated systems	No	Monte Carlo methods

Table 1.1: Existing ways of estimation of C_S for different systems

1.2 Relationship between Entropy and Mutual Information

1.2.1 Entropy: Statistical Approach

As described in the previous section, the main sources of uncertainty in the mathematical model are random variables (g_M, g_E, n_M, n_E). Therefore, in this thesis, the definition of uncertainty constructed for random variables will be used. This definition of uncertainty is used in communication difficulties, and other applied mathematical problems [21].

The *entropy* of a random variable X with density $p_X(x)$ is a function which attempts to characterize the unpredictability of this random variable [5]. There exist many ways to define this unpredictability. The definition for entropy as given by Shannon [5, 20] is:

$$H(X) = -\int_R log(p_X(x))p_X(x)dx. \tag{1.2}$$

For discrete random variables, entropy is defined as

$$H(X) = -\sum_i log(p_i)p_i, \tag{1.3}$$

where $p_i > 0$ are all positive probabilities for the values of X.

1.2.2 Mutual Information

Mutual information is a quantity that measures the relationship between two random variables that are sampled simultaneously. This measure provides how much information is communicated in one random variable about another and for this work it is very important to know how much does one random variable tells about another[2]. The definition of mutual information is given by conditional entropy between two random variables X and Y:

$$I(X;Y) = \sum_{x\in R_X}\sum_{y\in R_Y} P(x,y)log\left(\frac{P(x,y)}{P(x)P(y)}\right) = H(X) - H(X|Y). \tag{1.4}$$

[2]How accurate the distribution of the one variable by some information about the other variable could be predicted

In machine learning and deep learning for classification problems, the above definition is said to be the information gain. The relation described by Eqn.(1.4) is the main relation between entropy $H(X)$, conditional entropy $H(X|Y)$ and mutual information $I(X;Y)$. The entropy $H(X)$, conditional entropy $H(X|Y)$ and mutual information $I(X;Y)$ should satisfy the relation:

$$0 \leq I(X;Y) \leq H(X) \leq 1.$$

Eqn. (1.4) gives a good understanding of the nature of mutual information in two limit cases: $Y = X$ and independent X and Y. In the first case

$$H(X|Y) = H(X|X) = 0 \Longrightarrow I(X;Y) = H(X).$$

In the second case

$$P(x,y) = P(x)P(y) \Longrightarrow H(X|Y) = H(X) \Longrightarrow I(X;Y) = 0.$$

These two cases correspond to the conditions of total dependence and complete independence of random variables or in terms of the correlation between variables Y and Z: $\rho = \pm 1$ or $\rho = 0$. In classification problems, mutual information is called *information gain* [27] and characterizes the level of influence of the attributes by response variable, which describe class of the object.

1.3 Channel Capacity and Secrecy Capacity

1.3.1 Channel Capacity

To consider an arbitrary optimization problem, the target function (index), which depends on the parameters of the model needs to be determined. This indicator will be the difference between *channel capacities* for main channel and eavesdropper. So, one of core terms of this study is *channel capacities*, defined by the highest information rate (in units of information per unit time) that can be achieved with arbitrarily small error probability [5]. According

to Shannon - Hartley theorem [14] for channels with noise, throughput of this channel is the limiting transmission rate, which can be achieved with arbitrarily small probability of error.

Some authors consider error probability as the main characteristic of the system. For example, authors in [36] focus on a different index for secrecy of the channels, namely the probability of errors. In my research, this characteristic is closely related to the correlation for channels. This feature is more understandable as it shows the probability that the eavesdropper will not be able to decode the received message.

Main task in [25] is finding the upper bound of the decoding error for MIMO systems in Wyners wire-tap channel setting. Authors in [25] show that decoding error in the system satisfies the relation:

$$P_{error} \leq exp\left(-nE_r\right),$$

where P_{error} is the probability of error, n is length of the message, E_r is Gallagers random coding exponent.

One of the main tasks of my thesis is maximizing the main channel reliability by choosing "optimal parameters" of the system. Using Eqn(1.4), only one parameter of X – which is density (or mass function) $P(x)$ of the random variable X can be defined. It is intuitively clear that the reliability of the channel increases only by changing the properties (distribution) of X, that is

$$C_S(X) = \sup_{P(x)\in\mathcal{P}} I(X;Y), \tag{1.5}$$

where $\mathcal{P}$ is the class of the densities (mass functions) of the random variable X. In terms of the SNR P, let us define class $\mathcal{P}$ of the possible distributions in terms of covariance matrix of the input signal X:

$$\mathcal{P} = \left\{P(x) : Tr(cov(X)) \leq P\right\},$$

where $P(x)$ is the distribution of the random variable X, $cov(X)$ is the covariance of the random variable X, $Tr(A)$ is the trace of the matrix A.

1.3.2 Secrecy Criterion – Secrecy Capacity

Using the definition from Eqn(1.5), one can interpret the reliability of the system (or secrecy criterion) depicted in Fig.1.1 as a maximization of the capacity of the main channel ($X \to Y$), taking into account the minimization of the channel capacity of the second channel ($X \to Z$), which is the same as maximizing the difference between the channel capacities for the legitimate and eavesdropper channels.

Hence, the main task is maximizing information rate in *Legitimate channel* ($X \to Y$) with minimizing information rate in *Eavesdropper channel* channel ($X \to Z$).

Using the definition given from Eqn.(1.5), the secrecy capacity can be defined as

$$C_S = \sup_{P(x)\in\mathcal{P}} (I(X;Y) - I(X;Z)) \tag{1.6}$$

where $\mathcal{P}$ is the class of the densities (mass functions) of the random variable X. In fact, this formula defines maximization of the difference between the channel capacities of two channels (main and eavesdropper). Channel capacity is given by the following:

$$I(X;Y) = \frac{1}{2} log(det(I + H'\Sigma H))$$

where H is the channel gain, Σ is the covariance matrix of input signal X:

$$cov(X) = E((X - EX)'(X - EX))$$

Note that these equations of the channel capacity define the same result for SI* system, but different result for MI* systems [3].

Now to explain this concept on a concrete example, which is based on Fig. 1.1. Assume that the legitimate channel ($X \to Y$) is the channel between Alice and Bob and eavesdropper channel ($X \to Z$) is channel between Alice and Eve. Suppose, Alice wants to send message

[3] SI* systems means SISO and SIMO systems;
MI* systems means MISO, MIMO, MaMIMO systems.

to Bob maintaining confidentiality of message from Eve. By this description, Bob is the legitimate receiver and Eve is the eavesdropper.

The idea of Alice is to move information at the highest possible rate with high secrecy. Perfect secrecy is obtained when Eve fails to decode any confidential information without taking into account the computing power available. The concept of perfect secrecy precludes use of any cryptographic technique, because such techniques fail when the eavesdropper has infinite computing power. Is there any way to obtain perfectly secret communication in existence of an eavesdropper with infinite computing power? The answer is "yes" and it follows from the information-theoretic approach of achieving secret communication. The 'catch' is that Alice has to send information at a lower rate satisfying the secrecy constraint. For example, consider a very basic wire-tap channel. Assume that both channels are fixed; the point to point capacity of the legitimate channel is 5 bits per channel use and eavesdropper channel is 2 bits per channel use. The fundamental information of the theoretic results state, that a coding scheme can be constructed for perfectly secret communication if rate of the code, i.e., the rate of communication, occurs less than the difference of the capacities of the channels, which is 3 bits per channel use for previous case. The plan of constructing such coding scheme is to include noise in the encoding process to confuse the eavesdropper.

1.4 Information Theoretic Secrecy: Theory & Real World Problems

The main consideration with each theory is the assumptions on which the theory is based. In this case, all the main assumptions are based on the mathematical model given by Eqn.(1.1). By assumption, the model is linear and the noise in two channels have normal (Gaussian) distribution. One important simplification of the mathematical model in Eqn.(1.1) is that the channel gains are constants, and therefore do not depend on each other. As described above, channel capacities of legitimate and eavesdropper channels do not depend on the other channel. Its model corresponds to the case $\rho = 0$ in terms of correlation.

To solve another problem, the assumption about fixture of the channel gains should be changed. Assume that channel gains are correlated random variables with joint distribution

$f(h_1, h_2)$, where dimension of the vector h_1 corresponds to the dimension of the matrix g_M, dimension of the vector h_2 is the dimension of the matrix g_E, respectively.

The main tool for better understanding of the problem is modification of the mathematical model of the system. It can be done as follows:

- By generalization of the properties of random additive noises n_M and n_E.
- By generalization of the properties of channel gains g_M and g_E.

For this study, using the second option with generalization of the properties of channel gains g_M and g_E. There exist many works [8, 9, 35, 37, 38, 39, 41, 42] which use generalization by second option. Using the same generalization of the model in Eqn. (1.1), assuming that channel gains possess the following property:

$$(g_M, g_E) \sim f(h_1, h_2), \tag{1.7}$$

where $f(h_1, h_2)$ is the density over Euclidean space $R^{n(m+k)}$. Note that this description of the problem is more realistic than the constant case of g_M and g_E. All advantages of this approach will be discussed in the next section.

1.5 Correlation of Channel Gains

The main assumption about density $f(h_1, h_2)$ for calculation is given by:

$$f(h_1, h_2) = (2\pi)^{-N} det(\Sigma)^{-\frac{1}{2}} e^{-\frac{1}{2}(h-\mu)'\Sigma^{-1}(h-\mu)}, \tag{1.8}$$

where Σ is a covariance $n(m+k) \times n(m+k)$ matrix for μ – $n(m+k)$ vector, which defines average values of each parameter,

$$N = \frac{n(m+k)}{2}.$$

In particular for $n = m = k = 1$, matrix Σ and vector μ is given by:

$$h = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}, \mu = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}, \Sigma = \begin{pmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix},$$

where ρ is the correlation between channel gains g_M and g_E.

Consider density $f(h_1, h_2)$ for $n = m = k = 1$ with covariance matrix

$$\Sigma = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}.$$

The density $f(h_1, h_2)$ changes for different values of correlation coefficient shown in the Fig.1.2 below. For better understanding of the changes of secrecy capacity as function of ρ, consider the next representation of the channel gain g_E:

$$g_E = \mu_2 + \rho(g_M - \mu_1) + \sqrt{1 - \rho^2} g_A,$$

where $g_A \sim N(0, 1)$ is one dimensional normal distributed random variable with zero mean and variance $\sigma^2 = 1$. Now, assume that $\rho \to 1$. In this case

$$g_E \approx \mu_2 - \mu_1 + g_M.$$

Here we use next fact about distribution of g_E by known value of g_M:

$$g_E | g_M \sim N(\mu_2 - \rho(\mu_1 - g_E), (1 - \rho^2)\sigma^2).$$

Therefore $\mu_2 - \mu_1 > 0$ and it implies that

$$g_E - g_M \approx \mu_2 - \mu_1 > 0$$

Now assume that probability that $\mu_1 < 0$ and $\mu_2 < 0$ is about 0. Using these facts, we

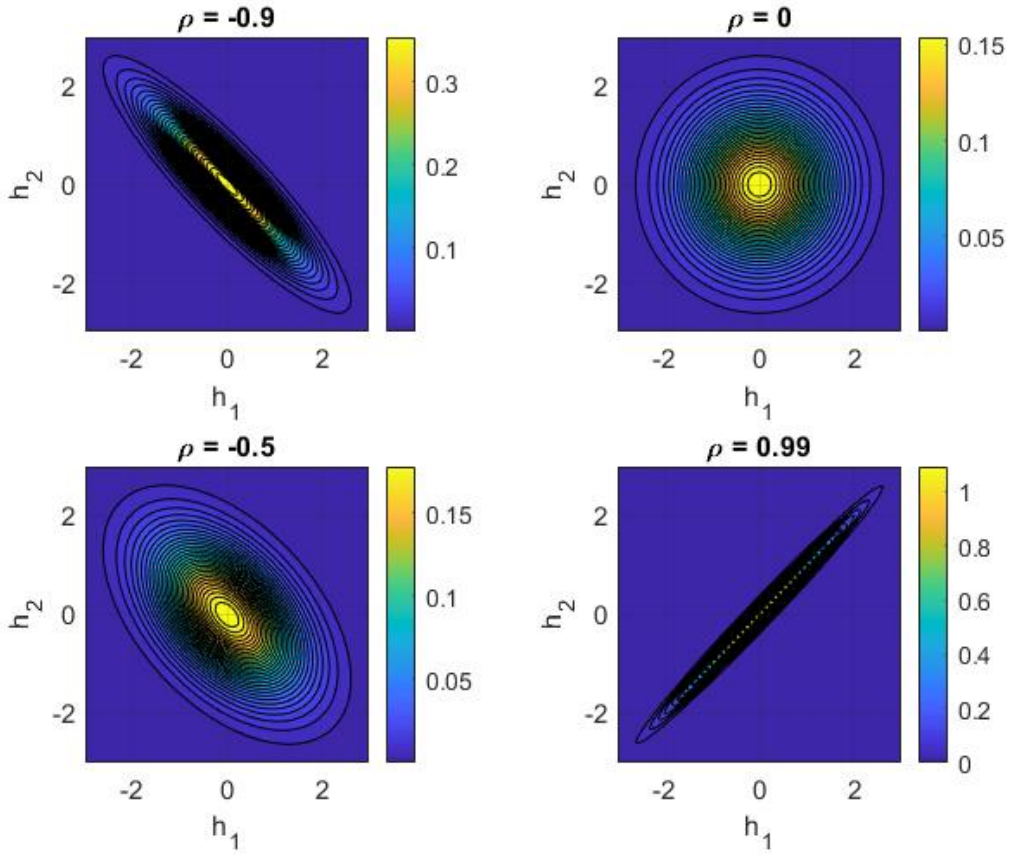

Figure 1.2: The joint density $f(h_1, h_2)$ plot for different values of correlation coefficient $\rho = -0.9, -0.5, 0, 0.99$.

get

$$(I(X;Y) - I(X;Y))^+ = \frac{1}{2}(log(1 + g_M^2 R) - log(1 + g_E^2 R)) = 0$$

Using this fact, simple conclusion in the case $\mu_2 - \mu_1 > 0$ is obtained

$$C_S = 0.$$

For a general case, the number of correlation parameters is $M = \frac{n(m+k)(n(m+k)-1)}{2}$:

$$\rho = (\rho_1, ..., \rho_M).$$

The number of correlations between elements of the channel gains g_M and g_E are

$$M_b = n^2 mk.$$

For simplification of the mathematical part, it can be assumed that elements in the two channels are independent meaning that the matrix Σ can be represented in the next form

$$\Sigma = \begin{pmatrix} diag(\sigma_1^2(M), ..., \sigma_{nm}^2(M)) & Corr \\ Corr' & diag(\sigma_1^2(E), ..., \sigma_{nk}^2(E)) \end{pmatrix}, \tag{1.9}$$

where $diag(\sigma_1^2, ..., \sigma_l^2)$ is $l \times l$ diagonal matrix with diagonal elements $\sigma_1^2, ..., \sigma_l^2$, $Corr$ is covariance matrix between elements of the channel gains g_M and g_E.

1.6 Main Results & Contributions

Main results of this thesis is reducing the task of finding the secrecy capacity with correlated channel gains using Eqn. (1.8) to the task of solving of the partial differential equations. Different LOS scenarios are simulated for identifying the scenarios where good secrecy is possible. The basic methods for finding secrecy capacity at present are statistical methods (*Monte Carlo methods*) [41, 45] that require the execution of a large number of operations (iterations). In this way, the speed of the algorithm is significantly reduced.

In this research, the use of differential equations in partial derivatives to find the secrecy capacity for SISO & MIMO systems is proposed. This approach greatly reduces the number of operations for calculations of secrecy capacity. This approach has some common ideas with work [32], but the authors of this work consider the deterministic case (g_M and g_E). The novelty of work [32] considers the impact of small variations in channel gains on the secrecy rate of a wiretap channel, in which it is assumed that imperfect channel knowledge is available at the transmitter. Hence, the main result of is focused in considering the secrecy capacity with varying channel gains. The main results are formulated in Theorem 1, in which the increment of secrecy capacity is defined as a function of the increments of g_M and

g_E:

$$\Delta C_S = \frac{g_M P}{g_M^2 P + \sigma_M^2}\Delta g_M - \frac{g_E P}{g_E^2 P + \sigma_E^2}\Delta g_E + o(max(\Delta g_M, \Delta g_E)), \tag{1.10}$$

where $\Delta C_S = C_S(g_M + \Delta g_M, g_E + \Delta g_E) - C_S(g_M, g_E)$. Using this approach, the authors construct an algorithm for calculating secrecy capacity, which is based on the following formula:

$$C_S(g_M + \Delta g_M, g_E + \Delta g_E) \approx C_S(g_M, g_E) + \frac{g_M P}{g_M^2 P + \sigma_M^2}\Delta g_M - \frac{g_E P}{g_E^2 P + \sigma_E^2}\Delta g_E.$$

A more statistical model, which is considered in this study, secrecy capacity is the function from 3 main parameters:

$$C_S = C_S(\rho, \mu, \Sigma).$$

Using properties of the expectation and properties of density of the multivariate normal distribution, it is proved that secrecy capacity C_S satisfies the next first order *partial differential equation (PDE)*:

$$\frac{\partial C_S}{\partial \rho} + \sum_{i=1}^{n(m+k)} u_i(\rho, \mu, \Sigma)\frac{\partial C_S}{\partial \mu_i} = u_0(\rho, \mu, \Sigma)C_S, \tag{1.11}$$

where $\frac{\partial y}{\partial x}$ is partial derivative of the function y by variable x. Using this equation, it is easy to estimate the values of SC in every finite region of the set parameters (ρ, μ, Σ). For uniqueness of the solution, it is necessary to determine the boundary conditions. In this case, these conditions are most easily determined for the following parameter values:

$$\mu_i = 0; \rho = 0.$$

For defining the boundary conditions, results of the work [32] can be used. Also, boundary values for C_S can by used by Monte Carlo method or some other estimations.

Consider estimation of the secrecy capacity, based on Eqn.(1.11). Assume that $\mu \in R^2$,

and the correlation parameter ρ is fixed. In this case, the last equation can be rewritten as

$$\frac{\partial C_S}{\partial \mu_1} + u_2(\rho, \mu, \Sigma)\frac{\partial C_S}{\partial \mu_2} = u_0(\rho, \mu, \Sigma)C_S.$$

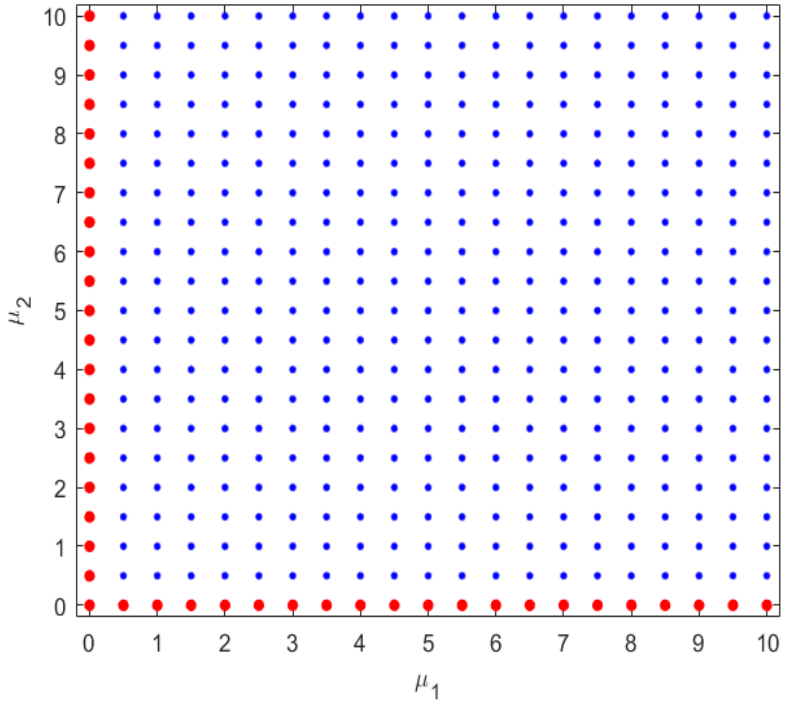

Figure 1.3: Grid of the points in the (μ_1, μ_2) plane for estimation of the secrecy capacity C_S

Fig.1.3 represents grid of the points on (μ_1, μ_2) plane for estimation of secrecy capacity C_S, where red dots indicate *boundary condition points*, blue dots indicate *interior points*. Values for secrecy capacity in the interior points can be calculated, using the estimation:

$$\frac{C_S(\rho, \mu) - C_S(\rho, \mu - \Delta_1\mu)}{\Delta\mu_1} + u_2(\rho, \mu, \Sigma)\frac{C_S(\rho, \mu) - C_S(\rho, \mu - \Delta_2\mu)}{\Delta\mu_2} \approx$$

$$u_0(\rho, \mu, \Sigma)C_S(\rho, \mu),$$

where

$$\Delta_1\mu = \begin{pmatrix} \Delta\mu_1 \\ 0 \end{pmatrix}, \Delta_2\mu = \begin{pmatrix} 0 \\ \Delta\mu_2 \end{pmatrix}.$$

Using this approximation, estimation of secrecy capacity C_S in points $(\mu_{1,i}, \mu_{2,j})$ is obtained by the next recurrent formula:

$$C_{S,i,j} = \frac{\Delta\mu_1^{-1} C_{S,(i-1),j} + \Delta\mu_2^{-1} u_{2,i,j} C_{S,i,j-1}}{\Delta\mu_1^{-1} + u_{2,i,j}\Delta\mu_2^{-1} - u_{0,i,j}} =$$

$$\frac{\Delta\mu_2 C_{S,(i-1),j} + \Delta\mu_1 u_{2,i,j} C_{S,i,j-1}}{\Delta\mu_2 + u_{2,i,j}\Delta\mu_1 - \mu_2\mu_1 u_{0,i,j}} \approx$$

$$\frac{\Delta\mu_2 C_{S,(i-1),j} + \Delta\mu_1 u_{2,i,j} C_{S,i,j-1}}{\Delta\mu_2 + u_{2,i,j}\Delta\mu_1}.$$

For complexity of the classical algorithm calculated by Monte Carlo method and the algorithm comparison, consider the parameters of the system: N – number of iterations in the Monte Carlo method, M_1 – number of points in μ_1 axis, M_2 – number of points in μ_2 axis. Using these parameters, the number of *flops* in the tow algorithm is received:

$$N_{Classical} = M_1 * M_2 * N,$$

$$N_{NewAlgo.} = (M_1 + M_2 - 1) * N + 3 * M_1 * M_2.$$

Thus, the developed algorithm has much faster performance under the condition

$$N \gg max(M_1, M_2).$$

1.7 Other Generalizations of the Main Model

H. Mahdavifar and A. Vardy [19], instead of constructing the vector $v \in (0,1)^n$ by setting $v_R = e$, $v_A = u$, and $v_B = 0$; set $v_R = e$, $v_A = u$, and $v_B = s$, where s is a fixed binary vector known a priori to all the parties. The authors then showed that there exists a choice

such that following qualities hold

$$\lim_{k\to\infty} \frac{I(U;Z)}{k} = 0, \lim_{n\to\infty} R_n = C(W^*) - C(W).$$

Mahdavifar's and A. Vardy's results also extend to discrete memory-less channels with non-binary input.

O.O. Koyluoglu, C.E. Koksal and H.E. Gamal [13] studied scaling behavior of the capacity of wireless networks under secrecy constraints. For extended networks with the path loss model, legitimate nodes and the eavesdropper were randomly placed in the network according to Poisson point processes. It is shown that when $\lambda_e = o\left((\log n)^{-2}\right)$, almost all nodes achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$, showing that securing the transmissions does not entail a loss in the per-node throughput for the model, where transmissions from other users are considered as noise at receivers. Their achievability argument is based on the novel secure multi-hop forwarding strategy where forwarding nodes are chosen such that no eavesdroppers exist in appropriately constructed secrecy zones around them and independent randomization is employed in each hop. Tools from percolation theory were used to establish the existence of a sufficient number of secure highways allowing for network connectivity. Finally, a time division approach was used to accomplish an end-to-end secure connection between almost all source-destination pairs.

With regards to digital communication, ref.[2] describes the transfer of bit-streams from one geographical location to another in different physical environments, such as wired pairs, coaxial cable, optical fiber and radio. The approach of this book is to extract the general principles underlying a range of media and applications and present them in a single structure. This has to do with the design of a variety of systems, including voice and video digital cellular phones, digital cable television, wireless local area networks, digital subscriber loop, metallic Ethernet, modems for voice-band data and satellite communications system.

As a continuation, it is interesting to get acquainted with work [22], which considers the use of artificial interference to reduce the likelihood that a confidential message transmitted

between two multi-antenna nodes will be intercepted by a passive interceptor. In this article, part of the transmit power is used to broadcast an information signal, which should be enough to guarantee a certain data rate for the intended receiver, and the remaining power is used to broadcast the artificial noise to mask the desired signal from a potential interceptor. A modified water filling algorithm has been proposed that balances the required transmit power with the number of spatial measurements sufficient to prevent the eavesdropping device from recognizing the transmitted information. There is also an increase in secrecy in modeling the proposed transmission scheme.

[30] discusses the use of artificial noise to reduce the likelihood that a message transmitted between two multi-antenna nodes will be intercepted by an undetected interceptor. The effectiveness of the relative signal-to-interference-plus-noise- ratio (SINR) of one transmitted data stream as a performance metric is shown.

In [31], the potential secrecy of composite listening channels was studied in the case of arbitrary sets of uncertainties (not necessarily countable or final states) and continuous input / output alphabets. The secrecy of a composite Gaussian MIMO listening channel was established while limiting the spectral norm on the interception channel. In this case, the channel does not have to be degraded.

The secrecy capacity is given in closed form:

$$C_S = \sum_{i:g_i>\lambda+\epsilon} \ln \frac{g_i}{\epsilon} + \sum_{i:g_i>\lambda+\epsilon} \ln \frac{2\epsilon + (\epsilon + g_i)z_i}{2g_i + (\epsilon + g_i)z_i},$$

where g_i are eigenvalues of the matrix of the channel to the legitimate receiver, fixed and known to the transmitter; $\epsilon > 0$;

$$z_i = max\left(\sqrt{1 + \frac{4\epsilon g_i}{(\epsilon + g_i)^2}\left(\frac{g_i - \epsilon}{\lambda} - 1\right)}\right) - 1, \lambda > 0.$$

It was shown that the property of saddle point is preserved, so that the composite bandwidth is equal to the worst-case value, and the transmission of signals over the worst channel reaches the composite bandwidth. Also, the isotropic interceptor shown is the worst

case, and the transmission of signals on the eigenmodes of the legitimate channel is optimal. The results apply to non-isotropic sets of uncertainties. It is shown that the presence of a maximum element in a set of uncertainties is sufficient for a saddle point to exist, so that the composite bandwidth is equal to the worst, and signaling on the worst channel reaches the bandwidth of the entire class of channels. In addition, these results are summarized to include legitimate channel uncertainty.

In [15], a method for ensuring secure communication by sending artificial noise by a transmitting antenna of a legitimate receiver is proposed. The path loss component in the far-field zone is considered and one concept of the field of wiretap channel secrecy is presented, that can be useful in developing security solutions at the physical level. Experimentally, by constructing a mathematical model, it was shown that the proposed method can provide high security in practical conditions, especially when the attacker's location is near the intended receiver. According to the authors, the proposed method can be combined with the existing method of forming a beam mask to further improve secrecy.

The Poisson process is an integral part in describing the functioning of communication networks. In article [34], the Poisson process of both secondary users and eavesdroppers is considered, and the effect of stochastic interference on fundamental limits of secure communication in a cognitive radio network is analyzed. A closed form for the secret capacitance between the main transmitter and receivers is obtained:

$$C_s = max\left\{log_2\left(1+\frac{P}{||x_i-x_j||^{\alpha}(W+I_P)}\right)-log_2\left(1+\frac{P}{||x_i-e^*||^{\alpha}(W+I_E)}\right),0\right\},$$

where $||x_i - x_j||$ is the distance between node x_i and node x_j , and α is the loss exponent of medium, P is the transmit power of primary nodes, I_P is the interference powers of P, I_E is the interference power of eavesdroppers from the cognitive users. Based on the theory of stochastic geometry, the influence of spatial Poisson process of primary and intercepting nodes on the secrecy capacity C_S and the probability of failure between a node and its neighbors are shown.

1.8 Thesis Outline

The thesis is devoted to the case when the channel gains are multi-normally distributed:

$$(g_M, g_E) \sim N(\mu, \Sigma).$$

The outline of the thesis is described as follows. Chapter 2 reviews the main systems related to the wireless transfer of information. We will consider two main wiretap transmission systems – Shannon's Cipher System and Wyner's Wiretap Channel. This chapter describes the difference between these systems and their mathematical models. Also the MIMO channel is introduced and methods are described for finding the main characteristics of MIMO systems. Another part of this section is the description of the influence of random perturbations in the MIMO system – n_M and n_E.

Chapter 3, partly, is an overview of methods of finding the secrecy capacity for SISO and MIMO systems with correlated channel gains g_M and g_E. Also, this chapter describes the main work devoted to these systems, where the channels have different distributions – exponential distribution, Rayleigh and Rician distributions, Gaussian and normal distributions. In this chapter a new method for finding the secrecy capacity with the use of Partial Differential Equations is considered. We find systems of partial differential equations for the secrecy capacity in the parameter areas μ_i, σ_j, ρ_k. Two algorithms for constructing systems of partial differential equations for SISO and MIMO systems in the areas of average values of channels gains $(\mu_1, ..., \mu_{n(k+m)})$ are considered.

Chapter 4 of the thesis is devoted to numerical examples, in which the interrelation between the secrecy capacity and the main parameters of the system $(\mu_i, \sigma_j, \rho_k)$ is analyzed in detail. A comparison of the Monte Carlo method and the method based on PDE, is carried out. Line of Sight (LOS) and Non-Line of Sight (N-LOS) scenarios are considered and graphs plotted similarly for Rayleigh and Rician distributions are evaluated. Chapter 4 is followed by the Conclusion and Future Research.

Chapter 2

History of Physical Layer Security & Related Works

2.1 Security at the Physical Layer

Wireless networks have become an indispensable part of our daily life, widely used in civilian and military applications. Security is a critical issue in wireless applications where people rely heavily on wireless networks for transmission of important/private information, such as credit card transactions or banking related data communications.

Most commonly used security methods rely on cryptographic techniques employed at the upper layers in the Open Systems Interconnection (OSI) model of a wireless network. If two users do not have their private key in the symmetric cryptosystem, a secure channel is required for the key exchange. Instead of using an additional channel, the physical layer methods can be employed here to distribute secret keys, to supply location privacy and to supplement upper-layer security algorithms. The application of physical layer security schemes makes it more difficult for attackers to decipher transmitted information.

The model described in Eqn.(1.1) consists of two main operations – $\oplus$ and $\otimes$. The first operation means the matrix multiplication by vector. Consider the operation $\oplus$ in sense of binary signals, where each single-input channel $X_i \in \{0, 1\}$. This assumption becomes a number of different input signals if equal,

$$N_X = 2^{|X|} = 2^n.$$

Also, the number of changed bytes after operation $\oplus$ is equal $N_X = 2^{|X|} = 2^n$ bytes by

assumption $Y_i, Z_i \in \{0, 1\}$. Using this assumption, one can conclude, that number of different matrices, which cover all possible cases, are

$$N_{X \Rightarrow Y} = 2^{m*2^n}.$$

In all calculations below, let's now use constraints about channel gains g_M and g_E, which are displayed in the form of a joint distribution of (g_M, g_E). This assumption greatly simplifies all mathematical calculations.

2.2 Physical Layer Security over the Years

The problem considered in this research was also considered in some other works [10, 35], which will be mentioned below in the literature review. The novelty of this work is the generalization of the model Eqn. (1.1) according to the assumption of the correlation between the channel gains g_M and g_E. As will be shown below, the presence of correlation for channels can lead to both increase and decrease of the secrecy capacity C_S. Therefore, it is not surprising that many works [40, 43] are devoted to the these systems – Shannons Cipher System, Wyner's Wiretap Channels, Gaussian Wiretap Channels, MIMO Wiretap Channels and Ma-MIMO Wiretap Channels.

2.2.1 Shannon's Cipher System

Consider the classical Shannons Cipher System, which is described as follows: let $X^n = (X_1, ..., X_n)$ be a message where each letter takes values on a finite set $\mathcal{X}$. This message is securely communicated from a transmitter to a receiver, both of which have access to a common secure key $K = U^k$ of purely k random bits independent of X^n. The transmitter computes the cryptogram

$$Y = Fun(X^n, U^k)$$

and sends it to the receiver over a public channel. The cryptogram may have variable length. The encryption function Fun is invertible for any fixed length of the message n. The

receiver, knowing Y and U^k, computes X^n. The functions Fun and Fun^{-1} are published.

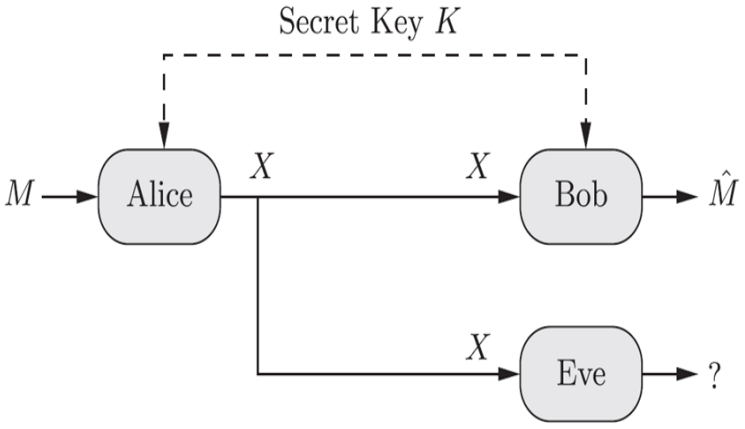

Figure 2.1: Shannon's model of a secrecy system.

This is an apt description of the Shannons Cipher System. Now, if a wiretapping attacker has access to the cryptogram, can attempt to identify the secure key without knowledge of the transmitter or the receiver. The attacker can use knowledge of the statistics of X^n.

Pioneer work in Shannon cipher system considered *Ciphertext-only attack*, where Eve (the eavesdropper) is assumed to have access to the ciphertext c. The target for Eve would be to try to recover the secret key k, the plaintext (original signal) X^n, or possibly some partial information about the plaintext. This is the weakest form of an attack that is considered in work [40].

2.2.2 Wyner's Wiretap Channel

Wyner introduced the notion of the wire-tap channel (Fig. 2.2) in study [43]. Alice wants to communicate a message X to Bob through a communication channel $V : X \to Y$. Eve also has access to what Alice transmits via a wire-tappers channel $W : X \to Z$ and the aim of Alice is to keep the message hidden from Eve while maximizing the rate of information transmitted to Bob.

$$Rate = \frac{1}{n} log(|M|)$$

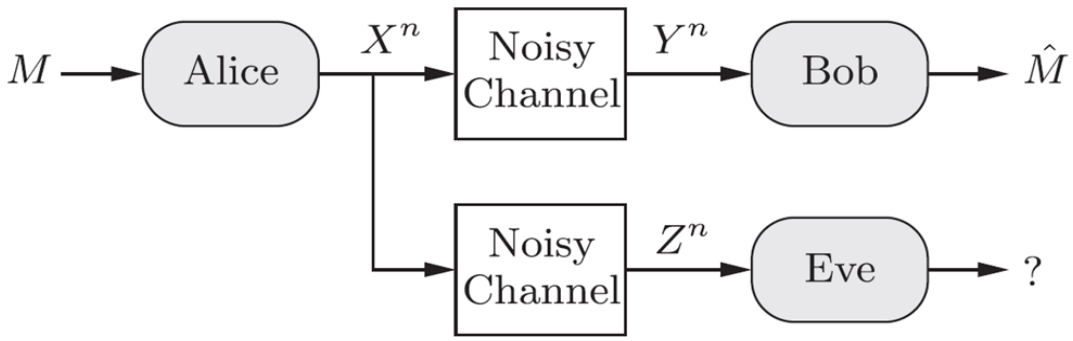

Figure 2.2: Wyner's wiretap channel

Wyner [43] showed that, given any input distribution P_X, Alice can communicate reliably to Bob at any rate up to

$$I(X;Y) - I(X;Z)$$

What is the difference between Shannon and Wyner models? The Shannon model sends an encrypted message X^n by some transformation[1], and the eavesdropper (Eve) tries to decrypt it, or decrypt only part of this message. In Wyner's model, the message is sent without encryption, but the eavesdropper channel is statistically worse than legitimate channel (Bob channel). Wyner proves that secure communication is possible in this case. Therefore, two main differences between Shannon and Wyner models can be specified:

- In Shannon cipher model, plain-text X^n is encrypted, the characteristics of the legitimate channel (Bob) and eavesdropper channel (Eve) are the same. Hence, statistical (probabilistic) characteristics of the signals Y and Z are the same, because $Y = Z$.

- Wyner's model assumes that the channels for Bob and Eve have different properties (statistical properties). This means that statistical (probabilistic) characteristics of the signals Y and Z are different.

[1] Defined by operations $\oplus$ and $\otimes$

2.2.3 Gaussian Wiretap Channel & the MIMO Wiretap Channel

In the previous two subsections, the systems without noise (without external influences) were considered. The main mathematical model of this work includes random additional noises n_M and n_E. These two additional terms change properties of the system and also as showed in other studies, difference in distribution of the terms n_M and n_E generate varying values for the secrecy capacity.

Main pioneer work related to wiretap channels describe single input single output (SISO) systems. But with the development of real systems, it became clear that considering these systems is not enough for real-life problems. Therefore, the main work from the last two decades is devoted to more complex systems, namely multi-input multi-output (MIMO) systems.

The account of noise in the system for the time being is an integral part of any model, since none of the created systems are perfect. Initial work related to the transmission of information [40, 43] did not take into account the presence of noise for two reasons:

1. At the time of the release of these two papers, the probability theory and random processes theory was not widely used in applied problems.

2. The authors of these works have considered idealized systems, which excluded the presence of other objects except Alice, Bob and Eve.

Ruoheng Liu and H. V. Poor [28] in paper "Multi-antenna Gaussian broadcast channels with confidential messages" investigated the secrecy capacity region of a generally non-degraded Gaussian BC with confidential messages for two users, where the transmitter has t antennas and each user has a single antenna. For this model, they have proposed a secret dirty-paper coding scheme and introduced a computable Sato-type outer bound. Furthermore, authors have proved that boundary of the secret dirty paper coding rate region is consistent with the Sato-type outer bound for multiple-antenna Gaussian BC, and hence,

have obtained the secrecy capacity region for the MGBC-CM.

$$C_S^{MG} = co\left\{\bigcup_{0\leq\beta\leq 1}\Sigma^{MG-2}(\beta)\right\}.$$

Unlike the single-antenna Gaussian BC-CM case, in which only the superior user can obtain confidential information at a positive secrecy rate, the result has illustrated that both users can achieve strictly positive rates with information-theoretic secrecy through a multiple-antenna Gaussian BC if attenuation vectors imposed on user 1 and user 2 are linear independent. Therefore, it becomes more practical and more attractive to achieve information-theoretic secrecy in wireless networks by employing multiple transmit antennas at the physical layer.

The authors of [45] investigated security of the physical layer of a system with multiple inputs and multiple outputs, consisting of one source and one destination in the presence of an interceptor, where each node is equipped with several antennas. Two schemes for selecting a transmitting antenna (optimal antenna selection and sub-optimal antenna selection) are considered, which work depending on whether the source has information about state of the global channel as the main channel and the channel that is being listened to. For performance comparison, a standard space-time transmission scheme is considered. The expressions in a closed form for the probability of zero secrecy capacity for the space-time transmission, optimal antenna selection and sub-optimal antenna selection schemes in conditions of Rayleigh fading are obtained. It is shown that the generalized order of secrecy diversity of the space-time transmission, sub-optimal antenna selection and optimal antenna selection schemes are the product of the number of antennas at source and destination:

$$d_{OAS} = d_{SAS} = MN_d,$$

where M and N_d represent the number of antennas at source and destination, respectively. It has been experimentally shown that the optimal antenna selection scheme is superior to both the sub-optimal antenna selection scheme and the space-time transmission scheme in

terms of probability of zero secrecy, confirming the safety benefits of using optimal choice of antennas against eavesdropping.

2.3 Importance of the Available CSI at Transmitter

Channel state information (CSI) is a collection of properties of a communication link. This information describes how a signal propagates from the transmitter to receiver and represents different effects of: scattering, fading, and power decay with distance. CSI makes it possible to adapt transmissions to current channel conditions, which is crucial for achieving reliable communication with high data rates in MIMO systems.

In general, the CSI can divided by two levels:

- Instantaneous CSI (or short-term CSI) defined by current channel conditions;
- Statistical CSI (or long-term CSI) defined by statistical characterization of the channel, calculated over a long-term period.

It should also be noted that all information about the channel is concentrated on the parameters g_M, g_E, n_M and n_E. As it is noted in the introduction, the systems belong to one of two types:

- Full Channel CSI: In this case, the exact values of the parameters g_M, g_E are known. Hence, these parameters have constant matrices.
- Partial Channel CSI: In this case, consider a system under uncertainty (partial information), namely assuming that the parameters are not constants, but are random variables with some distribution.

Most of the real-world systems belong to the second type, since, it is impossible to accurately determine parameters of the system. In this case, uncertainty of the system lies in the assumption given by Eqn.(1.8).

A. Mukherjee and A. L. Swindlehurst [23] have presented beam-forming based approaches for improving the secrecy of wireless communications between two multi-antenna nodes

$$\overline{Q}_{int} = E\{H_{ba} z' z'^H H_{ba}^H + n_b n_b^H\}.$$

The algorithms allocate transmit power in order to achieve a target SINR for a desired user, and then broadcast the remaining available power as artificial noise in order to disrupt interception of the signal by a passive eavesdropper. The proposed approaches rely heavily on availability of accurate CSI, and their performance can be quite sensitive leading to imprecise channel estimates. As a result, the authors conducted a detailed second-order perturbation analysis in order to precisely quantify the effects of inaccurate CSI. Simulations were used to demonstrate validity of the analysis, and to illustrate the sensitivity of algorithms that depend on precise CSI. To reduce impact of CSI errors, Mukherjee and Swindlehurst proposed two robust beam-forming schemes that are able to recover a large fraction of the SINR lost due to channel estimation errors. These techniques were shown to perform very well for moderate CSI errors, but ultimately a large enough channel mismatch can eliminate the secrecy advantage of using articial noise.

2.4 Literature Review

Consider now the main results, which are related to calculation C_S in the models described above.

Main goal of [12] is defining secrecy capacity for MIMO systems with complex-value matrices g_M and g_E. Also, authors of this work have considered complex-valued noises n_M and n_E – assuming n_M, n_E are independent $CN(0, I)$ processes[2]. For solving SC, the authors have used generalized eigenvalues of two matrices (g_M, g_E), which are defined as solutions of the equation

$$det(g_M - \lambda g_E) = 0$$

[2] $CN(0, I)$ is a complex-valued Gaussian process with average 0 and covariance matrix I

with corresponding eigenvectors. Main results of the article are focused on finding SC on limit case ($P \to \infty$). For example, the authors proved that limit value of secrecy capacity for $P \to \infty$ is approximately equal

$$C_S \approx C_0(P) + \sum_{\sigma_j > 0} log(\sigma_j^2) + O(1),$$

where σ_j is generalized singular values of the (g_M, g_E) problem. Also, the authors have considered different cases for rank of the matrices g_M and g_E and proven that in some cases C_S depends only on full-rank sub-matrices g'_M and g'_E. This is a very informative result for a reducing partial-information system to a full-rank system.

The main focus of study [17] is MIMO systems, which can be described by complex-valued generalization of the system given by Eqn.(1.1). Principal results of the work are based on the novel global optimization algorithm called branch-and-bound with reformulation and linearization technique. For simplification of the problem, authors have used the linearization of $log(x)$:

$$log(x) = \sum_{i \in Ind} I_i(x)(a_i x + b_i),$$

where a_i, b_i are some constants, Ind is a subset of indexes. Using this method, authors reduce the problem to a corresponding linear problem, which can also be obtained from Taylor series:

$$log(1 + x) = \sum_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}.$$

The results, obtained in [17] can be used for numerical calculation of SC, but not for contained closed form of SC.

Authors of the work [26] have described the general state of the problem of finding the secrecy capacity for different types of systems (SISO, MISO, MIMO) and define main ways for finding the SC estimations for each of these systems. Authors have shown the existence of the closed form for secrecy capacity only for two types of the system – SISO and SIMO systems. Also, authors have used different definitions for the channel capacity for AWGN

channel:

$$I(X) = log(det(I + \Sigma g'_M g_M)).$$

This representation changes the calculation of secrecy capacity, because

$$log(det(I + \Sigma g'_M g_M)) \neq log(det(I + g'_M \Sigma g_M)).$$

Thus, one can conclude that the closeness of secrecy capacity also depends on the form in which its value is calculated.

The main work of [44] is the assessment of secrecy capacity for SISO systems. In Theorem 2 of this work, a closed form of secrecy capacity for a MISO system with uncorrelated noise is given, which has the form

$$C_{S,MISO} = \sum_{i=1}^{M} C_{S,SISO}(i),$$

where $C_{S,SISO}(i)$ is value of secrecy capacity between uncorrelated sub-channels (SISO subsystems). The authors of these study have shown that the MIMO system with uncorrelated noise can be considered as several unconnected SISO systems. At the same time, the authors found a closed form of secrecy capacity for these systems. Also, the authors of this work have considered the case of uncorrelated g_M and g_E and shown that the value of C_S for SISO system in limit case for $P \to \infty$ can be estimated as

$$C_S \approx \frac{P}{2} \frac{Eg_M^2}{E(g_M + g_E)}.$$

Using the notation about joint distribution of g_M and g_E, this relation can be rewritten in the form

$$C_S \approx \frac{P}{2} \frac{\sigma_1^2 + \mu_1^2}{\mu_1 + \mu_2},$$

where $g_M \sim N(\mu_1, \sigma_1^2), g_E \sim N(\mu_2, \sigma_2^2)$.

F. Oggier and B. Hassibi [24] considered the problem of computing perfect secrecy

capacity of a multiple antenna channel, based on a generalization of the wire-tap channel to a MIMO broadcast wire-tap channel. The model was described by the following broadcast channel

$$Y = g_M X + n_M, \quad Z = g_E X + n_E,$$

where Y, n_M and Z, n_E are respectively $k \times 1$ vectors. Besides, F. Oggier and B. Hassibi have solved the optimization problem

$$\min_{A} \max_{K_X} \overline{I}(X; Y|Z)$$

by computing optimal $\overline{A}$ in a closed form expression, and by showing that optimal $\overline{K}_X$ is low rank.

T. Liu and S. Shamai [18] presented an alternative characterization using a channel enhancement argument. They considered a canonical version of the channel (vector Gaussian wiretap channel)

$$y_r[m] = x[m] + w_r[r], \quad y_e[m] = x[m] + w_e[m],$$

where $x[m]$ is the real input vector of length t, $w_r[m]$ and $w_e[m]$ are additive Gaussian noise vectors with zero mean and covariance matrices K_r and K_e, respectively, and are independent across the index m. The noise covariance matrices K_r and K_e are assumed to be positive definite. T. Liu and S. Shamai proved that, if there exists a positive semi-definite matrix, then the secrecy capacity of a degraded vector Gaussian wiretap channel can be written as

$$C = \frac{1}{2} \log det \left(I + K_x^* K_r^{-1} \right) - \frac{1}{2} \log det \left(I + K_x^* K_e^{-1} \right).$$

The characterization relies on an extreme entropy inequality recently proved in the context of multi-antenna broadcast channels, and is directly built on the physical intuition regarding the optimal transmission strategy in this communication scenario.

G. Geraci et al [7] proposed a linear precoder for the down-link of a multi-user MIMO system with multiple users that potentially act as eavesdroppers. The proposed precoder is

based on regularized channel inversion (RCI) with a regularization parameter α and power allocation vector chosen in such a way that the achievable secrecy sum-rate is maximized. The authors considered worst-case scenario for multi-user MIMO system, where the transmitter assumes users to co-operate to eavesdrop on other users

$$R_s = \sum_{k=1}^{K} \left[\log_2 \left(1 + \frac{|h_k^+ w_k|^2}{\gamma\sigma^2 + \sum_{j \neq k} |h_k^+ w_j|^2|} \right) - \log_2 \left(1 + \frac{||H_{\overline{k}} w_k||^2}{\gamma\sigma^2} \right) \right]^+ .$$

They derive the achievable secrecy sum rate and obtain closed-form expression for the optimal regularization parameter α_{LS} of the precoder using large-system analysis. Authors showed that the RCI precoder with α_{LS} outperforms several other linear precoding schemes, and it achieves a secrecy sum-rate that has same scaling factor as the sum-rate achieved by optimum RCI precoder without secrecy requirements. Geraci et al proposed a power allocation algorithm to maximize the secrecy sum-rate for fixed α. They then extend the algorithm to maximize the secrecy sum-rate by jointly optimizing α and the power allocation vector. The jointly optimized precoder outperforms RCI with α_{LS} and equal power allocation by up to 20 percent at practical values of the signal-to-noise ratio and for 4 users and 4 transmit antennas.

In [4], the new analytical and closed expressions for the probability of a strictly positive secrecy capacity and a lower bound for secure outage probability for the recently proposed $\kappa - \mu$ fading model were presented. In particular, analytical expressions were obtained for i.i.d. channel coefficients without parameter limitations. Analytical and closed-form expressions were tested by reducing to known particular cases and Monte-Carlo simulations. Since the proposed $\kappa - \mu$ fading model is a very general statistical model that includes many well-known distributions, in the article, the authors obtained new equations that can be used to characterize the secrecy of several different attenuation channels and calculating the probability of failures in wireless systems subject to co-channel interference and background noise, and calculation of the probability of failures in scenarios with limited interference. The utility of new formulations has been illustrated by examining the probability of strictly

positive secrecy capacity and a lower bound of secure outage selectivity based on actual channel measurements conducted for a diverse range of wireless applications such as cellular device-to-device, peer-to-peer, vehicle-to-vehicle and body-centric fading channels.

2.5 Summary

Secrecy capacity is one of the most important indicators that characterizes the reliability of the MIMO[3] system. However, at present, there are few major problems that prevent the calculation of this indicator to be simplified:

- Absence of a closed form for secrecy capacity C_S for the MIMO system.
- Absence of a closed form for secrecy capacity C_S for an arbitrary system with correlated channels.

The absence of a closed form for secrecy capacity causes the construction of methods for approximation of C_S. Most works [8, 9, 35, 37, 42] use the Monte Carlo method for this aim. However, this method, as a statistical method, is very slow. Therefore, other methods should be used to improve the results. The following table lists the main methods used to evaluate C_S.

[3]Or SISO, SIMO, MISO systems

Study	**System**	**Description**
Zang et al [44]	Uncorrelated MIMO and correlated SISO	Estimate $C_{S,MIMO}$ of MIMO system by $C_{S,SISO}$ of the SISO subsystems. Find estimation of the SISO system in terms of moments of g_M and g_E in limit case $P \to \infty$
Sedighizad et al [32]	Uncorrelated SISO	Estimation of ΔC_S by Δg_M and Δg_E. Novel approach for estimation of C_S by DE
Schaefer et al [31]	Uncorrelated MIMO	Find closed form of the C_S for composite Gaussian MIMO listening channel with specific form of channel gains g_M and g_E
Shu et al [34]	Uncorrelated MIMO	Considered effect of stochastic interference on the fundamental structure of the C_S in MIMO system
Liu & Poor [28]	Uncorrelated MIMO	Define upper and lower bounds for C_S by computable Sato-type outer bounds
Khisti & Wornell [12]	Uncorrelated MIMO	Estimation of the C_S by singular values of (g_M, g_E) in limit case $P \to \infty$
Li & Petropulu [16]	Uncorrelated MISO	Find a closed form of C_S for MISO system with additional conditions for channel gains

Table 2.1: Main results of estimation of C_S for different system

Chapter 3

Fading Gaussian Wiretap Channel with Correlation of Channel Gains

3.1 Non-Convexity of the Secrecy Capacity Expression

The main task of finding the optimal distribution between channels in the MIMO system is to maximize Eqn.(1.6). For systems considered in this research, the given problem can be rewritten in the following form:

$$C_S = \frac{1}{2} \sup_{tr(\Sigma) \leq P} (log(det(I + g'_M \Sigma g_M)) - log(det(I + g'_E \Sigma g_E))), \tag{3.1}$$

Let's define the optimization problem by matrix Σ, under the constraint $tr(\Sigma) \leq P$. The above Eqn.(3.1) is related to Non-Convex optimization problems. Thus, it is impossible to use standard methods of convex optimization for finding the solution for a given task. In addition, the closed form of the solution can only be found in critical cases for $k = m = 1$ or $n = 1$.

J. Li, A. Petropulu [16] have investigated the problem of finding the optimal input covariance matrix that achieves secrecy capacity subject to a power constraint. For general cases, the authors derive the necessary conditions for the optimal solution consisting of a set of equations. For the case in which transmitter has two antennas, the derived necessary conditions can result in a closed form solution. If the difference is indefinite and has all negative eigenvalues except one positive eigenvalue, they prove that the optimal input covariance matrix has rank one and can be obtained in closed form. For other cases, Li and Petropulu prove that the solution is a fixed point of mapping from a convex set to itself and

provide an iterative procedure to search for it.

MIMO network is a more complicated system and there is no closed form for determination of secrecy capacity for this system. In this case, authors have found many different ways to estimate SC for MIMO systems. One of the most used methods is the Monte Carlo method, which allows to determine precisely the secrecy capacity. But it should be noted that this method, although it is the most effective for MIMO systems, has a low efficiency if used for Massive MIMO systems (Ma-MIMO).

3.2 Bounds on Secrecy Capacity over Correlated Fading Channels with Full CSI

As noted in the previous section, for MIMO systems, there is no closed form for secrecy capacity. Therefore, in this case, one can either find estimation of the secrecy capacity using statistical methods (for example, the Monte Carlo method) or build bounds of the secrecy capacity, using properties of the function *log* and determinant of the matrix. Let's consider a few results, which corresponds to finding Upper Bound for MIMO systems with correlated gains for different regimes. One of the simplest of these bounds can be found from the relations:

$$log(1+x) \sim x, x \to 0.$$

$$log(1+x) \sim log(x), x \to \infty;$$

Using these simple relations, the estimation for SC for critical values of SNR ($SNR \to 0$ or $SNR \to \infty$) can be built. In the first case from Eqn. (3.1)

$$C_S \approx \sup_{tr(\Sigma) \leq P} (det(g'_M \Sigma g_M) - det(g'_E \Sigma g_E)).$$

In the second case

$$C_S \approx \sup_{tr(\Sigma)\leq P} (log(det(g'_M \Sigma g_M)) - log(det(g'_E \Sigma g_E))).$$

Main aim of [8] is the calculation of SC for correlated channels with exponential and Rayleigh distributions. For the exponential distribution C_S is calculated in closed form for $P \to \infty$:

$$C_S^{lim}(exp) = \frac{1}{2} log\left(-\frac{4(1-\rho)\Phi(u)}{\kappa u}\right),$$

where $\Phi(u)$ is given in [8]. The same result for $P \to \infty$ is given for Rayleigh distribution:

$$C_S^{lim}(Ray) = log(1+\kappa) + log\left(\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{\rho\kappa}{(1+\kappa)^2}}\right).$$

The authors of the study [9] have got the same results as the authors of the work [8] about limit distribution for $P \to \infty$ for exponential and Rayleigh distribution.

The research [37] considers correlated Rayleigh distribution, and the authors define secrecy capacity by next relation:

$$C_S = E(log(1+\gamma_M P(\gamma_M, \gamma_E)) - log(1+\gamma_E P(\gamma_M, \gamma_E))),$$

where

$$P(\gamma_M, \gamma_E) = \begin{cases} \left[0.5\sqrt{\psi\left(\frac{4}{\lambda}+\psi\right) - 0.5\phi}\right]^+, \text{ if } \gamma_E > 0, \\ \left[\frac{1}{\lambda} - \frac{1}{\gamma_E}\right], \text{ if } \gamma_E = 0, \\ 0, \text{ otherwise,} \end{cases}$$

where $\psi = \frac{1}{\gamma_E} - \frac{1}{\gamma_M}$, $\phi = \frac{1}{\gamma_E} + \frac{1}{\gamma_M}$. The authors of this research have defined the upper bound limits for secrecy capacity of correlated Rayleigh distribution.

In the research [39], authors have defined secrecy capacity for log-normal correlated

channels. In this case, authors prove that limit secrecy capacity for $P \to \infty$ is defined as

$$C_S^{lim} = \frac{Q}{\xi}[F_Y(y)]_{\mu_E}^{\infty},$$

where constants Q, ξ and function $F_Y(y)$ are defined in the paper.

Note that the papers [8, 9, 35, 37, 38] describes SISO systems. The research [41] describes case of the vectors' g_E and g_M normal distribution. In this case the distribution of vectors' g_E and g_M have χ^2 distributions. Hence, the authors of this paper have calculated results for the SISO system with correlated χ^2 distributions. Also, the authors have not got a closed form for secrecy capacity, but defined C_S as a series. This result can be used for estimation of C_S by finite sum.

The main achievement of the research [9] is the calculation of boundaries for the secrecy capacity for MIMO system with correlated ergodic fading channels at high SNR. This paper is a continuation of work [10], in which the authors in detail have described the bounds for realizations of complex Gaussian random processes g_M and g_E. In particular, they have proved that the closed form for upper bound of CS for limit case $P \to \infty, \rho \to 1$ exists and can be expressed as

$$\lim_{\rho \to 1} C + P(k, \rho) = \begin{cases} log(k), k > 1, \\ 0, k \leq 0, \end{cases}$$

where k is defined by fraction of two channels' average values:

$$k = \frac{Eg_M}{Eg_E}.$$

The main result of this study shows a relation between secrecy capacity for SISO systems for different values of ρ in the limit case $P \to \infty$:

$$(1 - \rho)C_S(k, 0) \leq C_S(k, \rho) \leq C_S(k, 0).$$

This result can be chosen only for high regime SNR, because for low regime SNR and when

$|\rho| < 1$ by definition of the joint distribution

$$C_S(k, \rho) > 0 \quad \forall k.$$

S. Shafiee, N. Liu and S. Ulukus [29] determined the secrecy capacity of the 2-2-1 Gaussian MIMO wire-tap channel, which is characterized by Eqn.(1.1) by solving for the optimum joint distribution for the auxiliary random variable and the channel input in the Csiszar – Korner formula. They projected a lower bound on the secrecy capacity by evaluating the Csiszar-Korner formula for a specific selection of the auxiliary random variable and the channel input. However, for some case, authors have shown that the optimal transmission scheme is unit-rank, i.e., beam-forming is optimal. Shafiee, Liu and Ulukus showed the optimality of the proposed achievable scheme by constructing a tight upper bound that meets it

$$\max_{S \geq 0 : tr(S) \leq P} U(S, a)$$

for any a with $||a|| < 1$, where $U(S, a)$ is defined as

$$U(S, a) = \frac{1}{2} \log \frac{|I + N^{-1} \overline{H} S \overline{H}^T|}{(1 + g^T S g)}.$$

The upper bound is developed by considering the secrecy capacity of a channel where the eavesdroppers signal is given to the legitimate receiver. Even though this upper bound is well-defined for a general MIMO wire-tap channel, explicit estimation and tightening of this upper bound has been possible by restricting ourselves to the 2-2-1 case. For the lower-bound, by selecting a certain correlation structure for additive noises, they have shown that beam-forming is optimal for the upper bound as well. Furthermore, authors have shown that optimal beam-forming directions in the lower and upper bounds are the same. Finally, Shafiee, Liu and Ulukus have shown that two bounds meet yielding the secrecy capacity. Their derivation is specific to the 2-2-1 case and they have not been able to show that these lower and upper bounds meet in the general MIMO channel. This is because the unit-rank

(beam-forming) property of the optimum transmit matrices is essential in the derivations, while beam-forming is not likely to be the optimal strategy when the number of transmit and receive antennas is more than two.

E. Ekrem and S. Ulukus [6] characterized the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. They showed the achievable rate with a variant of dirty-paper coding with Gaussian signals

$$\sum_{k=1}^{m} \mu_k \Sigma_k^* - \sum_{k=1}^{m} \mu_k \overline{\Sigma}_k \geq 0.$$

Before reaching this result, the authors first visited the scalar case, and showed the necessity of a new proof for the converse. In particular, they showed that the extensions of existing converses for the Gaussian scalar broadcast channels fall short of resolving the ambiguity regarding the auxiliary random variables. E. Ekrem and S. Ulukus showed that, unlike the stand-alone use of the entropy-power inequality, the use of relationships either between MMSE and mutual information or between Fisher information and differential entropy resolves this ambiguity. Extending this methodology to degraded vector channels, they found the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel,

$$\Sigma_k \leq \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} K_i + \sum_k \right|}{\left| \sum_{i=1}^{k-1} K_i + \sum_k \right|} - \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} K_i + \sum_Z \right|}{\left| \sum_{i=1}^{k-1} K_i + \sum_Z \right|}, k = \overline{1, K},$$

where the union is over all positive semi-definite matrices $K_{i\,i=1}^{K}$ that satisfy

$$\sum_{i=1}^{K} K_i = S.$$

Once they obtained the secrecy capacity region of the degraded MIMO channel, they generalized it to arbitrary channels by using the channel enhancement method and some limiting arguments.

A scenario where a source node wishes to broadcast two confidential messages for two respective receivers via a Gaussian MIMO broadcast channel, while a wire-tapper also receives

the transmitted signal via another MIMO channel is considered by Bagherikaram, Motahari and Khandani [1]. They considered the secure vector Gaussian degraded broadcast channel and established its capacity region. Their achievable scheme was the secret superposition of Gaussian codes. Instead of solving a non-convex problem, the authors used the notion of an enhanced channel to show that secret superposition of Gaussian codes is optimal – convex hull of the closure of all (Σ_1, Σ_2) satisfying

$$\Sigma_1 \leq I(X;Y_1|U) - I(X;Z|U), \quad \Sigma_2 \leq I(U;Y_2) - I(U;Z).$$

for the joint distribution $P(u)P(x|u)P(y_1, y_2, z|x)$.

To characterize secrecy capacity region of the vector Gaussian degraded broadcast channel, they only enhanced the channels for legitimate receivers, and channel of the eavesdropper remained unchanged. Then, Bagherikaram et al have extended the result of the degraded case to the non-degraded case. The authors showed that the secret superposition of Gaussian codes along with successive decoding cannot work when the channels are not degraded and developed a Secret Dirty Paper Coding (SDPC) scheme and showed that SDPC is optimal for this channel. They investigated practical characterizations for the specic scenario in which the transmitter and the eavesdropper can afford multiple antennas, while both intended receivers have a single antenna. The authors characterized the secrecy capacity region in terms of generalized eigenvalues of the receivers' channel and the eavesdropper channel. For high SNR they showed that the capacity region is a convex closure of two rectangular regions.

The research [3] is devoted to integral representations for finding the density and distribution function for the class of multi-dimensional Rayleigh and Rician distributions with a generalized correlation structure:

- Rayleigh CDF

$$F(r_1, r_2, ..., r_N) = \int_0^\infty \exp(-t) \prod_{k=1}^{N} \left[1 - Q\left(\frac{\sqrt{t}\sqrt{\rho_k^2}}{\sigma_k}, \frac{r_k}{\sigma_k} \right) \right] dt,$$

where ρ_k is the correlation coefficient, $\sigma^2 = \frac{1-\rho_k^2}{2}$, Q is 1st order Marcum Q-function;

- Rician CDF

$$F(\omega_1, \omega_2, ..., \omega_N) = \int_0^\infty \exp(-t) \exp(-(m_1^2 + m_2^2)) I_0\left(2\sqrt{t}\sqrt{m_1^2 + m_2^2}\right)$$

$$\times \prod_{k=1}^{N} \left[1 - Q\left(\frac{\sqrt{t}\sqrt{\rho_k^2}}{\sigma_k}, \frac{\omega}{\sigma_k}\right)\right] dt,$$

where m_1 and m_2 are means of two Gaussian distributions.

It should be noted that for this solution the computational complexity does not increase with the number of correlated RVs. In addition, CDF is computed directly and with one integration that does not require multiple (N for N-dimensional distribution) integrations to calculate CDF from PDF. To verify the accuracy of the theoretical results, numerical simulation results were used.

3.3 Expected Secrecy Capacity with Correlation of Channel Gains: Using PDE

3.3.1 SISO Systems

In this section, let's try to reduce the calculation of secrecy capacity using Partial Differential equations (PDE). Assume that the average value of SC is equal to

$$C_S = \int_{R^2} C(h_1, h_2) f(h_1, h_2) dh, \tag{3.2}$$

where $dh = dh_1 dh_2$, $f(h_1, h_2)$ is the joint density for channel gains (g_M, g_E), $C(h_1, h_2)$ is the secrecy capacity for system with given level of h_1 and h_2. Most authors use the following definition of the function $C(h_1, h_2)$:

$$C(h_1, h_2) = (log(1 + h_1' \Sigma h_1) - log(1 + h_2' \Sigma h_2))^+, \tag{3.3}$$

In this subsection for simplification, the case $n = m = k = 1$ is described.

Consider the case of normal distribution of the signals for

$$f(h_1, h_2) = \frac{1}{2\pi\sqrt{\det(\Sigma)}} e^{-\frac{1}{2}(h-\mu)'\Sigma^{-1}(h-\mu)}, \tag{3.4}$$

where

$$h = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}, \mu = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}, \Sigma = \begin{pmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix}. \tag{3.5}$$

Now let's find the partial derivative of C_S by $\mu_i, i = 1, 2$:

$$\frac{\partial C_S}{\partial \mu_i} = \int\limits_{R^2} C(h_1, h_2) \frac{\partial}{\partial \mu_i} f(h_1, h_2) dh. \tag{3.6}$$

Consider term under the integral :

$$\frac{\partial}{\partial \mu_i} f(h_1, h_2) = f(h_1, h_2) \frac{\partial}{\partial \mu_i} \left(-\frac{1}{2}(h-\mu)'\Sigma^{-1}(h-\mu) \right) =$$

$$-f(h_1, h_2) \left(I_i \Sigma^{-1}(h-\mu) \right) =$$

$$f(h_1, h_2) \left(I_i \Sigma^{-1}(\mu-h) \right),$$

$$\frac{\partial}{\partial \rho} f(h_1, h_2) = f(h_1, h_2) \frac{\partial}{\partial \rho} \left(-\frac{1}{2}(h-\mu)'\Sigma^{-1}(h-\mu) \right) =$$

$$f(h_1, h_2) \frac{\partial}{\partial \rho} \left(-\frac{1}{2(1-\rho^2)}(h-\mu)' \begin{pmatrix} \sigma_1^{-2} & -\rho\sigma_1^{-1}\sigma_2^{-1} \\ -\rho\sigma_1^{-1}\sigma_2^{-1} & \sigma_2^{-2} \end{pmatrix} (h-\mu) \right) =$$

$$f(h_1, h_2) \left(-\frac{\rho}{(1-\rho^2)^2}(h-\mu)' \begin{pmatrix} \sigma_1^{-2} & -\rho\sigma_1^{-1}\sigma_2^{-1} \\ -\rho\sigma_1^{-1}\sigma_2^{-1} & \sigma_2^{-2} \end{pmatrix} (h-\mu) \right) +$$

$$\frac{1}{1-\rho^2}(h_1-\mu_1)(h_2-\mu_2)\sigma_1^{-1}\sigma_2^{-1} f(h_1, h_2),$$

where vector I_i contains all 0^s except i-th elements, which is 1. Using these calculations,

$$\frac{\partial C_S}{\partial \mu_i} = \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) \left(I_i \Sigma^{-1} (\mu - h) \right) dh$$

$$= I_i \Sigma^{-1} \mu \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) dh - I_i \Sigma^{-1} \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) h dh$$

$$= I_i \Sigma^{-1} \mu C_S - I_i \Sigma^{-1} \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) h dh.$$

Note that,

$$\Sigma^{-1} = \frac{1}{(1-\rho^2)\sigma_1^2\sigma_2^2} \begin{pmatrix} \sigma_2^2 & -\rho\sigma_1\sigma_2 \\ -\rho\sigma_1\sigma_2 & \sigma_1^2 \end{pmatrix}$$

$$= \frac{1}{1-\rho^2} \begin{pmatrix} \sigma_1^{-2} & -\rho\sigma_1^{-1}\sigma_2^{-1} \\ -\rho\sigma_1^{-1}\sigma_2^{-1} & \sigma_2^{-2} \end{pmatrix}$$

and

$$I_1\Sigma^{-1} = \frac{1}{1-\rho^2} \begin{pmatrix} \sigma_1^{-2}, & -\rho\sigma_1^{-1}\sigma_2^{-1} \end{pmatrix},$$

$$I_2\Sigma^{-1} = \frac{1}{1-\rho^2} \begin{pmatrix} -\rho\sigma_1^{-1}\sigma_2^{-1}, & \sigma_2^{-2} \end{pmatrix}.$$

Assuming the parameters σ_1, σ_2, ρ are fixed. In this case,

$$\frac{\partial C_S}{\partial \rho} = 0.$$

There exists a function $g(\sigma_1, \sigma_2, \rho)$ for which

$$I_1\Sigma^{-1} \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) h dh +$$

$$g(\sigma_1,\sigma_2,\rho) I_2\Sigma^{-1} \int\limits_{R^2} C(h_1,h_2) f(h_1,h_2) h dh = 0. \tag{3.7}$$

Consider calculation of the value of function $g(\sigma_1, \sigma_2, \rho)$ by Eqn (3.7). Using this equation

and definitions of I_i, the next equality is obtained

$$I_1\Sigma^{-1}\int\limits_{R^2} C(h_1,h_2)f(h_1,h_2)hdh =$$

$$\frac{1}{1-\rho^2}\begin{pmatrix} \sigma_1^{-2}, & -\rho\sigma_1^{-1}\sigma_2^{-1} \end{pmatrix}(H_1,H_2)' =$$

$$\frac{1}{1-\rho^2}\left(\sigma_1^{-2}H_1 - \rho\sigma_1^{-1}\sigma_2^{-1}H_2\right),$$

where

$$H_i = \int\limits_{R^2} C(h_1,h_2)f(h_1,h_2)h_i dh.$$

Similar results are obtained for the second term from Eqn. (3.7):

$$I_2\Sigma^{-1}\int\limits_{R^2} C(h_1,h_2)f(h_1,h_2)hdh =$$

$$\frac{1}{1-\rho^2}\begin{pmatrix} -\rho\sigma_1^{-1}\sigma_2^{-1}, & \sigma_2^{-2} \end{pmatrix}(H_1,H_2)' =$$

$$\frac{1}{1-\rho^2}\left(-\rho\sigma_1^{-1}\sigma_2^{-1}H_1 + \sigma_2^{-2}H_2\right).$$

Substituting these values in Eqn.(3.7),

$$g(\sigma_1,\sigma_2,\rho) = \frac{\sigma_1^{-2}H_1 - \rho\sigma_1^{-1}\sigma_2^{-1}H_2}{\rho\sigma_1^{-1}\sigma_2^{-1}H_1 - \sigma_2^{-2}H_2} =$$

$$\frac{rH_1 - \rho H_2}{\rho H_1 - r^{-1}H_2}, \tag{3.8}$$

where $r = \sigma_2\sigma_1^{-1}$. Now, using this equation and Eqn. (3.6), it is easy to find PDE for C_S for different values of the averages (μ_1,μ_2).

$$\frac{\partial C_S}{\partial\mu_1} + g(\sigma_1,\sigma_2,\rho)\frac{\partial C_S}{\partial\mu_2} = I_i\Sigma^{-1}\mu C_S + g(\sigma_1,\sigma_2,\rho)I_i\Sigma^{-1}\mu C_S =$$

$$\frac{C_S}{1-\rho^2}\left[\mu_1\left(\sigma_1^{-2} - g\rho\sigma_1^{-1}\sigma_2^{-1}\right)\right] + \mu_2(g\sigma_2^{-2} - \rho\sigma_1^{-1}\sigma_2^{-1}).$$

Using the above relation, main PDE for C_S can be defined in the next form

$$\frac{\partial C_S}{\partial \mu_1} + g\frac{\partial C_S}{\partial \mu_2} = (u_1\mu_1 + u_2\mu_2)C_S, \tag{3.9}$$

where

$$\begin{cases} u_1 = \sigma_1^{-2} - g\rho\sigma_1^{-1}\sigma_2^{-1}, \\ u_2 = g\sigma_2^{-2} - \rho\sigma_1^{-1}\sigma_2^{-1}. \end{cases} \tag{3.10}$$

Now, consider the bound conditions for C_S. For this case, using the relation

$$\int\limits_{R^2} C(h_1, h_2) f_{\mu,\Sigma}(h_1, h_2)dh = \int\limits_{R^2} C(h_1 + \mu_1, h_2 + \mu_2) f_{0,\Sigma}(h_1, h_2)dh$$

Therefore, with $\mu_i \to \infty$ needed boundary values, the limit conditions can be calculated as

$$\lim_{\mu_1\to\infty} C_S = \lim_{\mu_1\to\infty} \int\limits_{R^2} C(h_1 + \mu_1, h_2 + \mu_2) f_{0,\Sigma}(h_1, h_2)dh$$

$$= \lim_{\mu_1\to\infty} \int\limits_{R^2} \log(1 + R(h_1 + \mu_1)) f_{0,\Sigma}(h_1, h_2)dh = \infty;$$

$$\lim_{\mu_2\to\infty} C_S = \lim_{\mu_2\to\infty} \int\limits_{R^2} C(h_1 + \mu_1, h_2 + \mu_2) f_{0,\Sigma}(h_1, h_2)dh$$

$$= \lim_{\mu_2\to\infty} \int\limits_{R^2} 0 f_{0,\Sigma}(h_1, h_2)dh = 0.$$

Hence, the main task for finding C_S can be rewritten in the form of PDE:

$$\begin{cases} \frac{\partial C_S}{\partial \mu_1} + g\frac{\partial C_S}{\partial \mu_2} = (u_1\mu_1 + u_2\mu_2)C_S; \\ \lim\limits_{\mu_1\to\infty} C_S = \infty; \\ \lim\limits_{\mu_2\to\infty} C_S = 0. \end{cases} \tag{3.11}$$

Note that the boundary conditions defined for the PDE in Eqn.(3.11) cannot be used,

because there multiple functions satisfying the Eqn.(3.11). For constricting the estimation of the solution, defined by Eqn. (3.11), the next form will be used:

$$\begin{cases} \frac{\partial C_S}{\partial \mu_1} + g\frac{\partial C_S}{\partial \mu_2} = (u_1\mu_1 + u_2\mu_2)C_S; \\ C_S|_{\mu_1=0} = b_2(\mu_2); \\ C_S|_{\mu_2=0} = b_1(\mu_1). \end{cases} \tag{3.12}$$

Now, consider an algorithm for the secrecy capacity C_S estimation for correlated channel gains g_M, g_E, the distribution of which is defined by Eqn. (3.4).

Algorithm 3.1

Step 1. Define grid of the points $\eta_{i,j} = (\mu_{1,i}, \mu_{2,j})$ where

$$\mu_{1,i} = \mu_{1,0} + step_1 * i;$$

$$\mu_{2,j} = \mu_{2,0} + step_2 * j.$$

Step 2. Calculate the values of H_i:

$$H_i = \int\limits_{R^2} C(h_1, h_2) f(h_1, h_2) h_i dh$$

for the bounds of the grid.

Step 3. Calculate value of the function g, defined in Eqn. (3.8).

Step 4. Define bound conditions for secrecy capacity C_S in the bounds of the grid – these are points $C_{S,i,0}$ and $C_{S,0,j}$, where

$$C_{S,i,j} = C_S(\eta_{ij}).$$

Step 5. Calculate the functions u_1 and u_2, defined in the Eqn. (3.10).

Step 6. Calculate estimation of the secrecy capacity by first equation in Eqn. (3.11). Using the estimation of derivative by finite difference in the points η_{ij}, the next estimation

is found:

$$C_{S,i,j} = \frac{step_2 C_{S,(i-1),j} + step_1 v_{2,i,j} C_{S,i,j-1}}{step_2 + v_{2,i,j} step_1 - step_1 step_2 v_{0,i,j}},$$

where

$$\begin{cases} v_0 = g; \\ v_2 = u_1\mu_1 + u_2\mu_2. \end{cases}$$

3.3.2 MIMO Systems

In previous subsection, SISO systems was considered. In this section, the case of MIMO system will be considered. For simplicity, consider the case of a system with

$$n = k = m = 2.$$

In this case matrix Σ have dimension 8×8 and is next form

$$\Sigma = \begin{pmatrix} \Sigma_M & \Sigma_{M,E} \\ \Sigma^{'}_{M,E} & \Sigma_E \end{pmatrix},$$

where matrices $\Sigma_M, \Sigma_{M,E}, \Sigma_E$ are next:

$$\Sigma_M = \begin{pmatrix} \sigma^2_{M,1} & 0 & 0 & 0 \\ 0 & \sigma^2_{M,2} & 0 & 0 \\ 0 & 0 & \sigma^2_{M,3} & 0 \\ 0 & 0 & 0 & \sigma^2_{M,4} \end{pmatrix}, \Sigma_E = \begin{pmatrix} \sigma^2_{E,1} & 0 & 0 & 0 \\ 0 & \sigma^2_{E,2} & 0 & 0 \\ 0 & 0 & \sigma^2_{E,3} & 0 \\ 0 & 0 & 0 & \sigma^2_{E,4} \end{pmatrix}$$

$$\Sigma_{M,E} = \begin{pmatrix} \rho_1\sigma_{M,1}\sigma_{E,1} & \rho_2\sigma_{M,1}\sigma_{E,2} & \rho_3\sigma_{M,1}\sigma_{E,3} & \rho_4\sigma_{M,1}\sigma_{E,4} \\ \rho_5\sigma_{M,2}\sigma_{E,1} & \rho_6\sigma_{M,2}\sigma_{E,2} & \rho_7\sigma_{M,2}\sigma_{E,3} & \rho_8\sigma_{M,2}\sigma_{E,4} \\ \rho_9\sigma_{M,3}\sigma_{E,1} & \rho_{10}\sigma_{M,3}\sigma_{E,2} & \rho_{11}\sigma_{M,3}\sigma_{E,3} & \rho_{12}\sigma_{M,3}\sigma_{E,4} \\ \rho_{13}\sigma_{M,4}\sigma_{E,1} & \rho_{14}\sigma_{M,4}\sigma_{E,2} & \rho_{15}\sigma_{M,4}\sigma_{E,3} & \rho_{16}\sigma_{M,4}\sigma_{E,4} \end{pmatrix}$$

Assume that the channel gains for any channel (except g_M and g_E) are uncorrelated, so

matrices Σ_M and Σ_E are diagonal matrices. Vector of average values for the channel gains g_M and g_E is $(\mu_1, ..., \mu_8)$, where μ_i is defined from next relation

$$E(g_M) = \begin{pmatrix} \mu_1 & \mu_2 \\ \mu_3 & \mu_4 \end{pmatrix}, E(g_E) = \begin{pmatrix} \mu_5 & \mu_6 \\ \mu_7 & \mu_8 \end{pmatrix}.$$

Hence, number of parameters in this MIMO system is

$$N = 8 + 8 + 16 = 24.$$

Using previous forms of μ, Σ and ρ, we can calculate partial derivatives of secrecy capacity C_S by all parameters:

$$\frac{\partial C_S}{\partial \mu_i} = \frac{\partial}{\partial \mu_i} \left(\int\limits_{R^8} C_S(h) f_{\mu,\Sigma}(h) dh \right) =$$

$$-\frac{1}{2} \int\limits_{R^8} C_S(h) f_{\mu,\Sigma}(h) \frac{\partial}{\partial \mu_i} \left((h-\mu)' \Sigma^{-1} (h-\mu) \right) dh =$$

$$\int\limits_{R^8} C_S(h) f_{\mu,\Sigma}(h) \left(I_i \Sigma^{-1} (h-\mu) \right) dh,$$

where I_i is vector which contain only 0^s except i^{th} position with value 1. Using definition of I_i, next relation is true:

$$I_i \Sigma^{-1} (h-\mu) = I_i \Sigma^{-1} H - C_S * (I_i \Sigma^{-1} \mu),$$

where vector H defined as in previous subsection:

$$H_i = \int\limits_{R^8} C_S(h) f(h) h_i dh, i = 1, ..., 8.$$

Now consider the construction of PDE as in previous subsection. First define functions

g_i, which depend from parameters $\sigma_k, k = 1, ..., 8$ and $\rho_j, j = 1, ..., 16$ for which

$$G'\Sigma^{-1}H = 0, \tag{3.13}$$

where vector $G = (g_1, ..., g_8)$. Eqn.(3.13) has more than 1 solution for MIMO system, hence we can use any of them. For example, consider next solution of Eqn. (3.13) in the form $G = (g_1, g_2, 0, ..., 0)$. Using this form of vector G, we get system of two linear equations with two unknown variables g_1 and g_2.

After defining vector G, it is easy to construct a system of PDE in the next form

$$\sum_{i=1}^{8} G_i \frac{\partial C_S}{\partial \mu_i} = G\Sigma^{-1}H - C_S * (G\Sigma^{-1}\mu) =$$

$$-C_S * (G\Sigma^{-1}\mu)$$

Using this equation, define estimation of the secrecy capacity C_S in the point $u_{i_1,...,i_8}$ in the space $\mu \in R^8$:

$$C_{S,k_1,....,k_8} * (G\Sigma^{-1}\mu) \approx -\sum_{i=1}^{8} G_i \frac{\Delta_i C_{S,k_1,....,k_8}}{\Delta_i}.$$

Using forward approximation of $\Delta_i C_{S,k_1,....,k_8}$[1], we get

$$C_{S,k_1,....,k_8} * (G\Sigma^{-1}\mu) \approx -\sum_{i=1}^{8} G_i \frac{\Delta_i C_{S,k_1,....,k_8}}{\Delta_i} =$$

$$-\sum_{i=1}^{8} G_i \frac{C_{S,k_1,....,k_8} - \delta_i C_{S,k_1,....,k_8}}{\Delta_i}.$$

Solving this equation by $C_{S,k_1,....,k_8}$:

$$C_{S,k_1,....,k_8} * \left(G\Sigma^{-1}\mu + \sum_{i=1}^{8} G_i \Delta_i^{-1} \right) = \sum_{i=1}^{8} G_i \frac{\delta_i C_{S,k_1,....,k_8}}{\Delta_i}. \tag{3.14}$$

[1]
$$\Delta_1 C_{S,k_1,....,k_8} = C_{S,k_1-1,k_2,...,i_8} - C_{S,k_1,k_2,...,k_8},$$
$$\Delta_2 C_{S,k_1,....,k_8} = C_{S,k_1,k_2-1,...,k_8} - C_{S,k_1,k_2,...,k_8}, ...$$

Algorithm 3.2

Step 1. Define grid of the points $\eta_{i,j} = (\mu_{1,k_1}, \mu_{2,k_2}, ..., \mu_{8,k_8})$, where

$$\mu_{j,k_j} = \mu_{j,0} + step_j * k_j;$$

Step 2. Calculate the values of H_i:

$$H_i = \int\limits_{R^8} C(h) f(h) h_i dh, i = 1, ..., 8.$$

for the bounds of the grid in the space R^8.

Step 3. Calculate value the elements of vector G from Eqn. (3.13).

Step 4. Define bound conditions for secrecy capacity C_S in the bounds of the grid – these are points $C_{S,k_1,...,k_8}$, where $min(k_1, ..., k_8) = 0$.

Step 5. Calculate estimation of the secrecy capacity in the point $(\mu_{1,k_1}, ..., \mu_{8,k_8})$, using the estimation of derivative by finite difference – Eqn. (3.14):

$$C_{S,k_1,....,k_8} = \left(G\Sigma^{-1}\mu + \sum_{i=1}^{8} G_i \Delta_i^{-1} \right)^{-1} \sum_{i=1}^{8} G_i \frac{\delta_i C_{S,k_1,....,k_8}}{\Delta_i}.$$

by solving system of the linear equations with unknown values $C_{S,k_1,....,k_8}$.

Chapter 4

Theoretical & Numerical Results

4.1 Expected Secrecy Capacity with Correlation of Channel Gains using Monte-Carlo Method

Consider one result for SISO system with correlated channel gains. Assume that the two channel gains g_M and g_E satisfy next relation

$$g_E = \rho g_M + \sqrt{1-\rho^2} Unc,$$

where ρ is correlation coefficient, Unc is some function (matrix valued function), which does not depend on g_M. Therefore, two critical cases ($\rho = \pm 1$) must give secrecy capacity 0. These theoretical conclusions are also confirmed by calculations made on basis of the Monte-Carlo method (Fig. 4.1). From Fig. 4.1, it is obvious that the maximal secrecy capacity is obtained for large values of SNR and small values of ρ.

As we see, the presence of correlation between channel gains can greatly vary the secrecy capacity. In Fig. 4.1, the secrecy capacity decreases if correlation coefficient between channel gains goes from $\rho = 0$ to $\rho = \pm 1$. In addition, the secrecy capacity is symmetric with respect to the line $\rho = 0$. This property of secrecy capacity is a simple corollary for the SISO systems for values averaging over zero. In addition, it will be shown that secrecy capacity depends on the parameters of the system – (ρ, μ, Σ) in the next section.

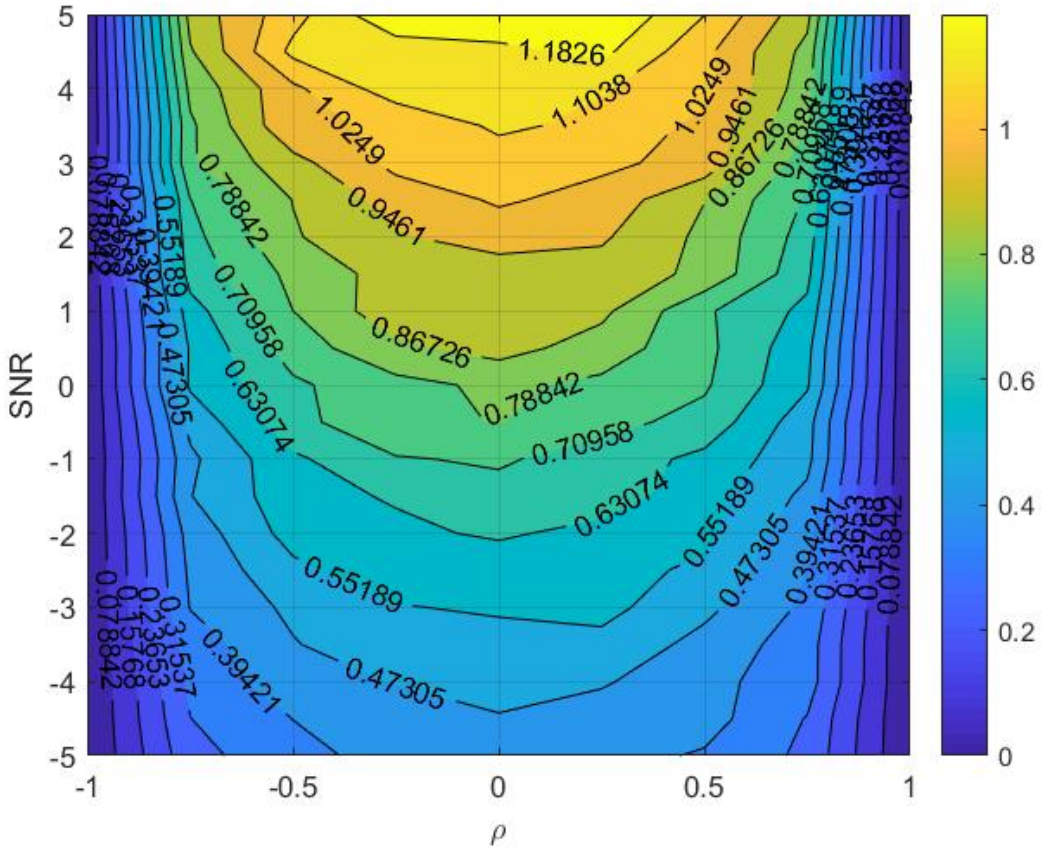

Figure 4.1: Contour plot of Secrecy Capacity as function of correlation ρ and SNR

Note that all the contour plots and graphs in this chapter are plotted using the color scale as dark blue to light yellow for ascending values of the Secrecy Capacity. Each plot has its own color bar and the limits for Secrecy Capacity are defined on this color bar.

4.2 Comparison of Expected Secrecy Capacity using Monte-Carlo method & PDE for Correlated Channel Gains

Consider the calculation result of the secrecy capacity C_S for SISO systems with the next parameters:

$$\sigma_1 = 1; \sigma_2 = 2;$$

$$\rho \in \{-1, -0.2, 0, 0.1, 0.8, 1\};$$

$$P = 1; step_1 = step_2 = 0.2;$$

$$\mu_1, \mu_2 \in [0, 10]; Iterations = 10^3.$$

From the Fig. 4.2 and Fig. 4.3, the difference between the approximations received of secrecy capacity for two solutions is not more than 10^{-3}. These results indicates the high accuracy of the proposed model (Eqn. (3.12)).

Also consider speed of the proposed algorithms for different number of iterations in the Monte-Carlo method. For this consider the times needed for calculating estimation of C_S by two methods for different number of iterations. From resulting Tab. 4.1, execution time

Number of iteration	Execution time MC (sec.)	Execution time PDE (sec.)
10^2	51	3
10^3	344	14
10^4	3225	147

Table 4.1: Execution time for MC and PDE algorithms

of the Monte-Carlo algorithm is much slower than the corresponding execution time for the algorithm using PDE. Therefore, there is no doubt that the described algorithm can be applied to higher dimensions ($n > 1$, $m > 1$, $k > 1$) with an increase in the efficiency than the classical Monte-Carlo algorithm. Also, we can calculate execution time for the Monte-Carlo method for number of iterations equal 10^5 – this time is approximately 13123 sec (about 3.5 hours). Difference operators have been applied only for the function $f_{\mu,\Sigma}$.

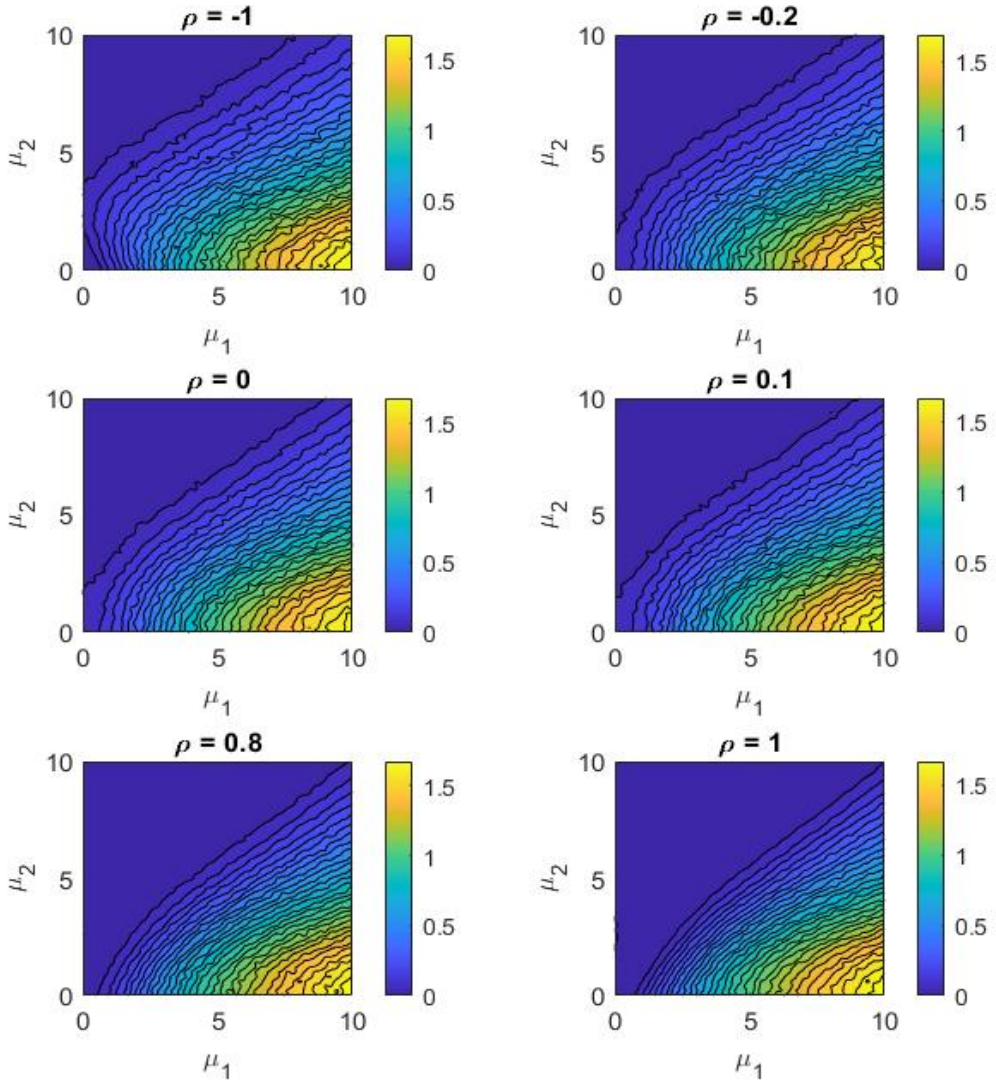

Figure 4.2: Contour plot of the secrecy capacity C_S as function of the parameters (μ_1, μ_2) calculated by MC method

It is also possible for the function $C(h_1, h_2)$ with the help of the next integration by substitution:

$$C_S = \int_{R^2} C(h_1, h_2) f(h_1, h_2) dh =$$

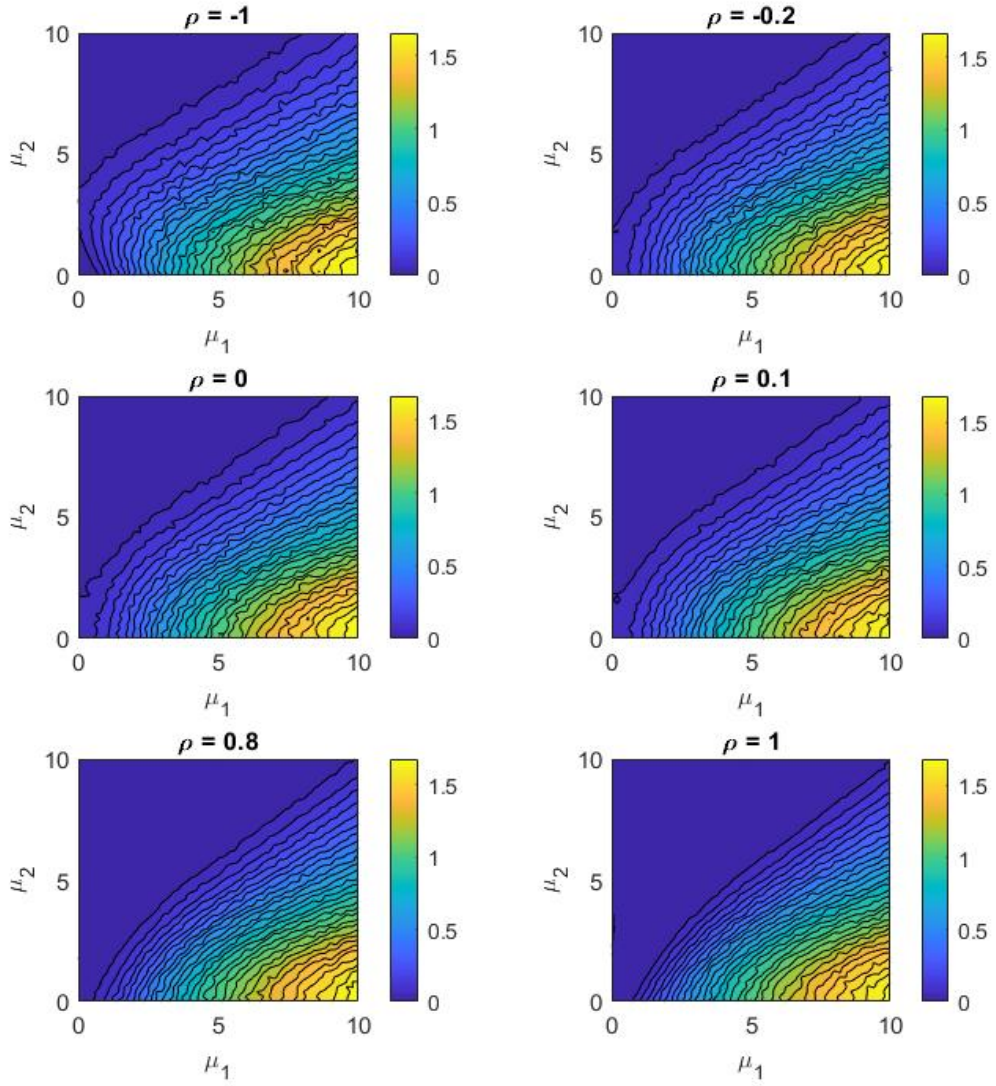

Figure 4.3: Contour plot of the secrecy capacity C_S as function of the parameters (μ_1, μ_2) calculated by PDE from Eqn. (3.12)

$$\int_{R^2} C(\varphi(u)) f(\varphi(u)) det(D(\varphi(u))) du,$$

where the substitution $h = \varphi(u)$ and Jacobian of the substitution $D(\varphi(u))$ are defined as

$$\begin{cases} h = \varphi(u) = \mu + \Sigma^{\frac{1}{2}} u \\ D(\varphi(u)) = \Sigma^{\frac{1}{2}} \end{cases},$$

where $\Sigma^{\frac{1}{2}}$ defines a square root from positive-defined matrix. Using this substitution, the next equality is true:

$$f(\varphi(u)) = f_{0,I}(u)$$

This means that the term $f(\varphi(u))$ does not depend on system parameters $par = (\rho, \mu_1, \mu_2, \sigma_1, \sigma_2)$. Hence,

$$\frac{\partial C_S}{\partial par_i} = \int\limits_{R^2} f(\varphi(u)) \frac{\partial}{\partial par_i} \left(C(\varphi(u)) det(D(\varphi(u)))\right) du$$

This trick helps to simplify the calculations, because

$$\frac{\partial}{\partial par_i} \left(C(\varphi(u))\right) det(D(\varphi(u)))$$

is a rational function.

Now consider the result for estimation of the value of secrecy capacity C_S as function from σ_1, σ_2 and ρ, where other parameters $(\mu_1, \mu_2) = (0, 0)$. Results of calculations we can see in the Fig. 4.4. As we can see from this figure, values of the secrecy capacity is almost same for values of correlation ρ near ± 1. This result respond for the same theoretical result about values of the secrecy capacity C_S. The other interesting result is that secrecy capacity increased for value $\mu = 0$ when $\rho \to 1$ and decreased when $\rho \to \pm 1$.

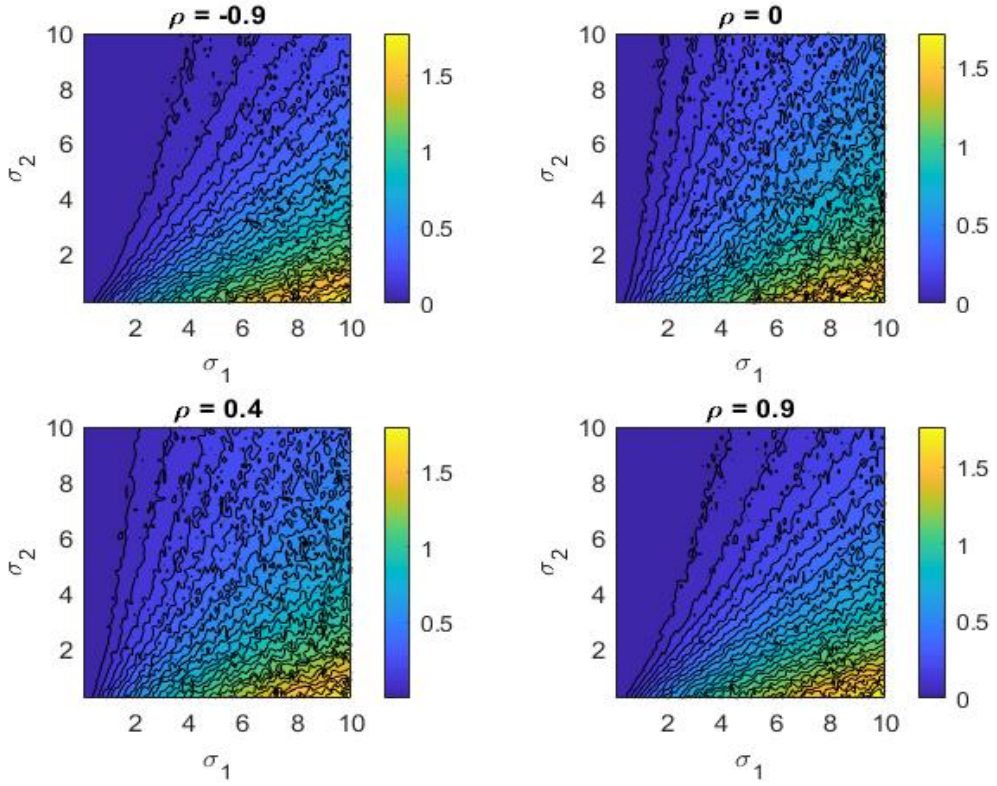

Figure 4.4: Contour plot of the secrecy capacity C_S as function of the parameters $(\sigma_1, \sigma_2) \in [0, 10]^2$ calculated by PDE

Now consider the different scenarios of line-of-sight propagation and how it affects the values for secrecy capacity C_S for 3 pairs of the parameters (μ_1, μ_2) with same values of the $(\sigma_1, \sigma_2) = (1, 1)$ with varying SNR to the receiver and constant SNR to the eavesdropper shown by Fig. 4.5 and Fig. 4.6 below.

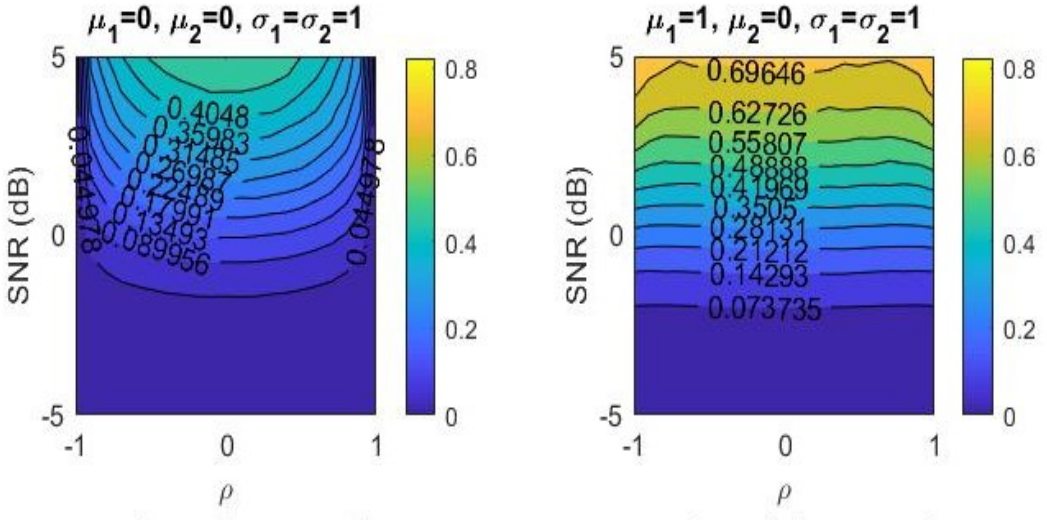

Figure 4.5: Contour plot of the secrecy capacity C_S as function of the parameters $(\rho, SNR) \in [-1, 1] \times [0, 5]$ for different values of (μ_1, μ_2) and for constant SNR at the Eavesdropper

These are the scenarios for the calculation of C_S when SNR to the legitimate receiver is varying. As we can see from Fig. 4.5, and Fig. 4.6, values of the secrecy capacity C_S have interesting relation with level of SNR. These relations also depend on other parameters of the system – $\mu_1, \mu_2, \sigma_1, \sigma_2$. From the three plots, the maximal values of secrecy capacity C_S for any given value of SNR for the legitimate receiver is near $\rho = 0$. This can also be seen in the Fig. 4.1. Even when the noise energy is better at the eavesdropper, we get a maximum Secrecy Capacity of around 0.32 when $\rho \to 0$ in Fig. 4.6 shown below.

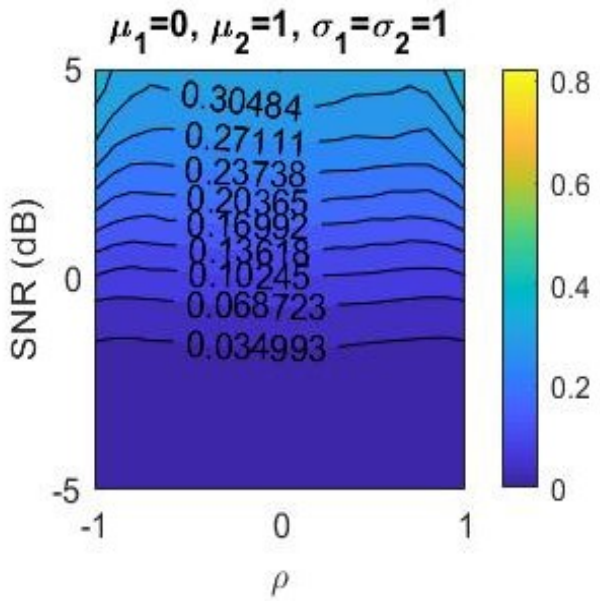

Figure 4.6: Contour plot of the secrecy capacity C_S as function of the parameters $(\rho, SNR) \in [-1, 1] \times [0, 5]$ for the values $(\mu_1 = 0, \mu_2 = 1)$ and for constant SNR at the Eavesdropper

Now, consider the below plot as an example, with both the receiver and the eavesdropper having N-LOS propagation which is shown in Fig. 4.7. The SNR is varied from $-5dB$ to $5dB$. It is observed that the contour plot is symmetrical and the secrecy capacity increases for when $\rho \to 0$ and goes to a maximum of around 0.6 and decreases symmetrically when $\rho \to \pm 1$. Hence, all the three plots show that secure communication is possible when the legitimate and eavesdropper channels have correlated gains when the SNR is varying at the legitimate receiver and constant at the eavesdropper.

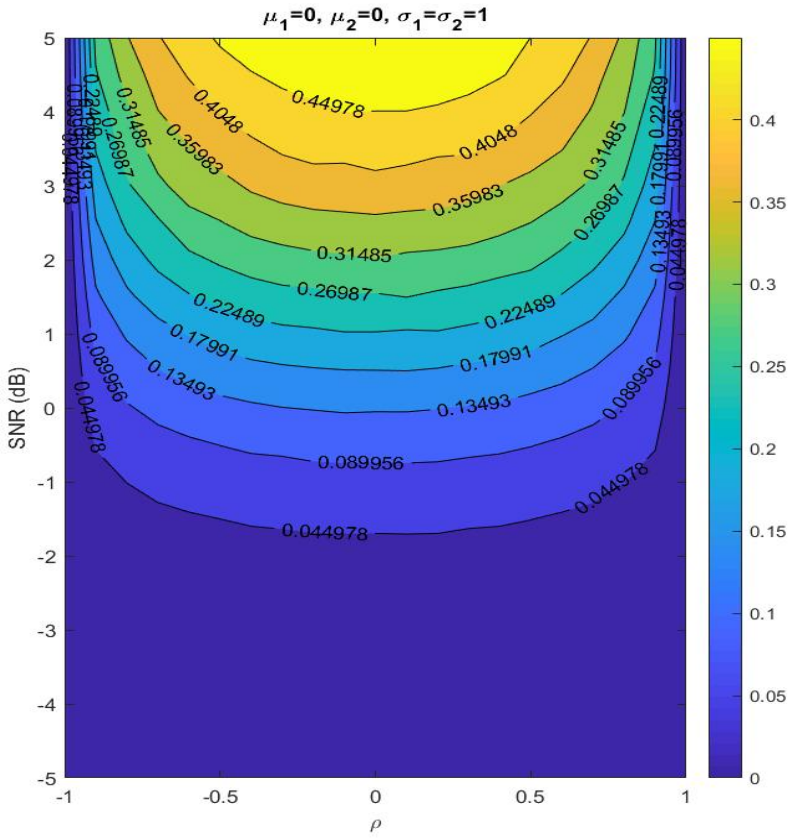

Figure 4.7: Contour plot of Secrecy Capacity as function of correlation ρ and signal-to-noise ratio SNR for N-LOS propagation with varying SNR at the receiver and constant SNR at the eavesdropper

Chapter 5

Conclusions

The Secrecy Capacity is determined for correlated channel gains for the main and eavesdropper channels in the Gaussian Wiretap channel. It was assumed that the system's secrecy capacity (Alice, Bob, Eve) is a continuously differential function from the system parameters: ρ_i – the coefficients of correlations between elements of channel gains g_M and g_E; the elements of the vector μ and the matrix Σ, which represent average values and covariance matrix of the channel gains (g_M, g_E), respectively. Under conditions of normal distribution of parameters (g_M, g_E), a system in partial differential equations for the secrecy capacity, which describes the changes of C_S in space of the parameters (ρ, μ, Σ), is obtained. The new algorithm has a higher speed than analog algorithms constructed on the classical statistical Monte Carlo methods.

Important scenarios in which there is line-of-sight and non-line-of-sight propagation are considered and numerically solved for the Secrecy Capacity for correlated channel gains. It was identified that secure communication is possible with correlation of channel gains and those scenarios were plotted.

5.1 Future Work

In the future works, it is planned to improve the results by considering additional scenarios using Rayleigh, Rician and exponential distributions. These scenarios form a much bigger picture when Delay-Doppler is considered for secure communication and how correlation of channel gains would help in achieving secure communication.

Additionally, it is planned to improve the results using other approximations of the solution of the partial differential equations by different schemes. Also, in this work, the explicit method was used for estimation of the solution of the partial differential equations. As a result, stability of the method depends from steps $step_i$. To solve the stability problem of the proposed approximation scheme, it would be better to apply implicit scheme[1], since the stability of the estimation will not depend on the values of the steps $step_i$.

The third direction for future research work is to consider the correlation between channel gains g_M and g_E and random additive terms n_M and n_E. In general, it is planned to consider the following dependence

$$n_M \sim N(0, \Sigma_M), \Sigma_M = \Sigma_M(g_M),$$

$$n_E \sim N(0, \Sigma_E), \Sigma_E = \Sigma_E(g_E)$$

Hence, the main task of the thesis is generalized by the assumption that magnitude of the noises n_M and n_E in the channels $X \Rightarrow Y$ and $X \Rightarrow Z$ depend on the channel gains. The main areas of future work will be to investigate the properties of the secrecy capacity in more general cases and to develop algorithms for estimation of the C_S for MIMO systems.

[1] Also known as Backward method

Bibliography

[1] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "The Secrecy Capacity Region of the Gaussian MIMO Broadcast Channel," in IEEE Transactions on Information Theory, vol. 59, no. 5, pp. 2673-2682, May 2013. doi: 10.1109/TIT.2012.2236972

[2] John R. Barry, Edward A. Lee, David G. Messerschmitt (2004). Digital Communication. 3rd ed. Springer

[3] N. C. Beaulieu and K. T. Hemachandra, "Novel Simple Forms for Multivariate Rayleigh and Rician Distributions with Generalized Correlation," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, 2010, pp. 1-6. doi: 10.1109/GLOCOM.2010.5683590

[4] N. Bhargav, S. L. Cotton and D. E. Simmons, "Secrecy Capacity Analysis Over κ μ Fading Channels: Theory and Applications," in IEEE Transactions on Communications, vol. 64, no. 7, pp. 3011-3024, July 2016. doi: 10.1109/TCOMM.2016.2565580

[5] T.M. Cover, J.A. Thomas (2006). Elements of Information Theory. John Wiley & Sons, New York.

[6] E. Ekrem and S. Ulukus, "The Secrecy Capacity Region of the Gaussian MIMO Multi-Receiver Wiretap Channel," in IEEE Transactions on Information Theory, vol. 57, no. 4, pp. 2083-2114, April 2011. doi: 10.1109/TIT.2011.2111750

[7] G. Geraci, M. Egan, J. Yuan, A. Razi and I. B. Collings, "Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding," in IEEE Trans-

actions on Communications, vol. 60, no. 11, pp. 3472-3482, November 2012. doi: 10.1109/TCOMM.2012.072612.110686

[8] H. Jeon, N. Kim, M. Kim, H. Lee and J. Ha, "Secrecy capacity over correlated ergodic fading channel," MILCOM 2008 - 2008 IEEE Military Communications Conference, San Diego, CA,https://www.overleaf.com/7556953629xjdjddrpxtvr 2008, pp. 1-7. doi: 10.1109/MILCOM.2008.4753256

[9] H. Jeon, N. Kim, J. Choi, H. Lee and J. Ha, "Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR," in IEEE Transactions on Information Theory, vol. 57, no. 4, pp. 1975-1983, April 2011. doi: 10.1109/TIT.2011.2112190

[10] Hyoungsuk Jeon, Namshik Kim, Minki Kim, Hyuckjae Lee and Jeongseok Ha, "Secrecy capacity over correlated ergodic fading channel," MILCOM 2008 - 2008 IEEE Military Communications Conference, San Diego, CA, 2008, pp. 1-7. doi: 10.1109/MILCOM.2008.4753256

[11] Hyoungsuk Jeon, Namshik Kim, Jinho Choi, Hyuckjae Lee and Jeongseok Ha, "Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR," in IEEE Transactions on Information Theory, vol. 57, no. 4, pp. 1975-1983, April 2011. doi: 10.1109/TIT.2011.2112190

[12] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple AntennasPart II: The MIMOME Wiretap Channel," in IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010. doi: 10.1109/TIT.2010.2068852

[13] O.O. Koyluoglu, C.E. Koksal and H.E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," in IEEE Transactions on Information Theory, vol. 58, no. 5, pp. 3000-3015, May 2012. doi: 10.1109/TIT.2012.2184692

[14] J. Lesurf. "Signals look like noise!". Information and Measurement, 2nd ed.

[15] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis," in IEEE Communications Letters, vol. 16, no. 10, pp. 1628-1631, October 2012. doi: 10.1109/LCOMM.2012.081612.121344

[16] J. Li, A. Petropulu, "Transmitter Optimization for Achieving Secrecy Capacity in Gaussian MIMO Wiretap Channels" in arXiv:0909.2622 [cs.IT], 2018.

[17] J. Liu, Y. T. Hou and H. D. Sherali, "Optimal power allocation for achieving perfect secrecy capacity in MIMO wire-tap channels," 2009 43rd Annual Conference on Information Sciences and Systems, Baltimore, MD, 2009, pp. 606-611. doi: 10.1109/CISS.2009.5054790

[18] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," in IEEE Transactions on Information Theory, vol. 55, no. 6, pp. 2547-2553, June 2009. doi: 10.1109/TIT.2009.2018322

[19] H. Mahdavifar and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes," in IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6428-6443, Oct. 2011. doi: 10.1109/TIT.2011.2162275

[20] J.L. Massey, "Guessing and entropy," Proceedings of 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, 1994, pp. 204-. doi: 10.1109/ISIT.1994.394764

[21] R. Muhamedyev, K. Yakunin, S. Iskakov, S. Sainova, A. Abdilmanova and Y. Kuchin, "Comparative analysis of classification algorithms," 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Rostov on Don, 2015, pp. 96-101. doi: 10.1109/ICAICT.2015.7338525

[22] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," 2009 IEEE 10th Workshop on Signal

Processing Advances in Wireless Communications, Perugia, 2009, pp. 344-348. doi: 10.1109/SPAWC.2009.5161804

[23] A. Mukherjee and A. L. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI," in IEEE Transactions on Signal Processing, vol. 59, no. 1, pp. 351-361, Jan. 2011. doi: 10.1109/TSP.2010.2078810

[24] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," in IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 4961-4972, Aug. 2011. doi: 10.1109/TIT.2011.2158487

[25] M. B. Parizi and E. Telatar, "On the secrecy exponent of the wire-tap channel," 2015 IEEE Information Theory Workshop - Fall (ITW), Jeju, 2015, pp. 287-291. doi: 10.1109/ITWF.2015.7360781

[26] H. V. Poor, R. F. Schaefer. "Wireless physical layer security", Proceedings of the National Academy of Sciences Jan 2017, 114 (1) 19-26; DOI: 10.1073/pnas.1618130114

[27] L. Rokach and O. Maimon, "Top-down induction of decision trees classifiers - a survey," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 35, no. 4, pp. 476-487, Nov. 2005. doi: 10.1109/TSMCC.2004.843247

[28] R. Liu and H. V. Poor, "Multi-antenna Gaussian broadcast channels with confidential messages," 2008 IEEE International Symposium on Information Theory, Toronto, ON, 2008, pp. 2202-2206. doi: 10.1109/ISIT.2008.4595381

[29] S. Shafiee, N. Liu and S. Ulukus, "Towards the Secrecy Capacity of the Gaussian MIMO Wire-Tap Channel: The 2-2-1 Channel," in IEEE Transactions on Information Theory, vol. 55, no. 9, pp. 4033-4039, Sept. 2009. doi: 10.1109/TIT.2009.2025549

[30] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, 2009, pp. 2437-2440. doi: 10.1109/ICASSP.2009.4960114

[31] R. F. Schaefer and S. Loyka, "The Secrecy Capacity of Compound Gaussian MIMO Wiretap Channels," in IEEE Transactions on Information Theory, vol. 61, no. 10, pp. 5535-5552, Oct. 2015. doi: 10.1109/TIT.2015.2458856

[32] M. Sedighizad, H. G. Bafghi and B. Seyfe, "Sensitivity of the secrecy capacity of a wiretap channel to the channel gains with imperfect channel information," 2017 Iran Workshop on Communication and Information Theory (IWCIT), Tehran, 2017, pp. 1-5. doi: 10.1109/IWCIT.2017.7947669

[33] S. Shafiee and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," 2007 IEEE International Symposium on Information Theory, Nice, 2007, pp. 2466-2470. doi: 10.1109/ISIT.2007.4557589

[34] Z. Shu, Y. Yang, Y. Qian and R. Q. Hu, "Impact of Interference on Secrecy Capacity in a Cognitive Radio Network," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Kathmandu, 2011, pp. 1-6. doi: 10.1109/GLOCOM.2011.6133652

[35] J. Si, Z. Li, J. Cheng and C. Zhong, "Secrecy Performance of Multi-Antenna Wiretap Channels With Diversity Combining Over Correlated Rayleigh Fading Channels," in IEEE Transactions on Wireless Communications, vol. 18, no. 1, pp. 444-458, Jan. 2019. doi: 10.1109/TWC.2018.2881140

[36] David Tse and Pramod Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005.

[37] M.Z.I. Sarkar and T. Ratnarajah, "Bounds on the secrecy capacity with diversity combining techniques," 2012 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, 2012, pp. 2847-2851. doi: 10.1109/WCNC.2012.6214287

[38] M.Z.I. Sarkar and T. Ratnarajah, "Enhancing Security in Correlated Channel With Maximal Ratio Combining Diversity," in IEEE Transactions on Signal Processing, vol. 60, no. 12, pp. 6745-6751, Dec. 2012. doi: 10.1109/TSP.2012.2213080

[39] M.Z.I. Sarkar and T. Ratnarajah, "Secrecy capacity over correlated log-normal fading channel," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, 2012, pp. 883-887. doi: 10.1109/ICC.2012.6363666

[40] C. Shannon. "Communication Theory of Secrecy Systems", Bell System Technical Journal, Vol. 28(4), 1949, pp. 656715.

[41] W. Xu, Z. Peng and S. Jin, "On Secrecy of a Multi-Antenna System with Eavesdropper in Close Proximity," in IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1525-1529, Oct. 2015. doi: 10.1109/LSP.2015.2411612

[42] Y. Du, S. Han, S. Xu and C. Li, "Improving Secrecy under High Correlation via Discriminatory Channel Estimation," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6. doi: 10.1109/ICC.2018.8422837

[43] A. D. Wyner. The wire-tap channel. Bell Systems Tech. Journal, 54(8):13551387, 1975.

[44] Li, Zang & Yates, Roy & Trappe, W. (2009). Secrecy Capacity of Independent Parallel Channels. 10.1007/978-1-4419-1385-21.

[45] J. Zhu, Y. Zou, G. Wang, Y. Yao and G. K. Karagiannidis, "On Secrecy Performance of Antenna-Selection-Aided MIMO Systems Against Eavesdropping," in IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 214-225, Jan. 2016. doi: 10.1109/TVT.2015.2397195